SECURITY INTELLIGENCE
REVIEW COMMITTEE

Amending the CSIS Act

Proposals for the Special Committee of the House of Commons 1989

Canada

SECURITY INTELLIGENCE
REVIEW COMMITTEE

Amending the CSIS Act

Proposals for the Special Committee of the House of Commons 1989

90-03316/

Security Intelligence Review Committee
365 Laurier Avenue West
P.O. Box 2430, Station D
Ottawa, Ontario
K1P 5W5

(613) 990-8441: Collect calls are accepted, and the switchboard is open from 7:30 a.m. to 6 p.m. Ottawa time.

© Minister of Supply and Services Canada 1989
Cat. No. JS71-1/1-1989
ISBN 0-662-56970-9

PREFACE

A special, all-party committee of the House of Commons, under the chairmanship of Blaine Thacker, M.P., has been established to review the *Canadian Security Intelligence Service Act* and the companion *Security Offences Act*.

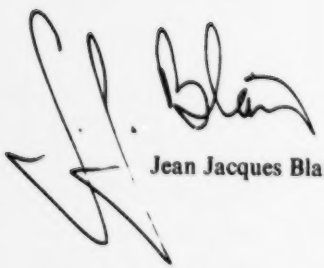
As members of the Security Intelligence Review Committee, Parliament's and the public's watchdog on the Service, we hope to contribute to the parliamentary committee's deliberations by putting forward specific suggestions, set out in these pages, and by appearing before it as witnesses.

After five years of experience, we believe that the CSIS legislation has generally worked quite well. As we said in our 1987-88 Annual Report, we continue to believe that the appropriate model for security intelligence in Canada is:

> A civilian agency whose mandate is spelled out in law rather than by executive order, with clear political and judicial control, and with independent review.

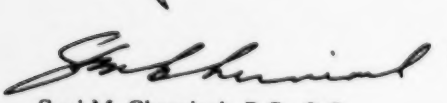
That is, of course, exactly what the *CSIS Act* was designed to create. Our suggestions are meant to improve the working of the *Act*, not to modify its basic design.

Ronald G. Atkey, P.C., Q.C.
Chairman

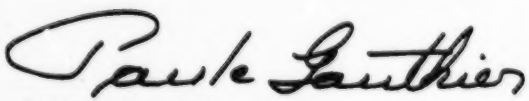


Jean Jacques Blais, P.C., Q.C.

Frank McGee, P.C.



Saul M. Cherniack, P.C., Q.C.



Paule Gauthier, P.C., Q.C.

Contents

The CSIS Mandate: "Threats to the Security of Canada" 1
Paragraph 2(d) (Domestic Subversion) 1
Paragraph 2(b) (Foreign Influenced Activities) 2
Overcoming Isolation 4
Grievance Procedures 5
Warrants 5
Devil's Advocate 7
Cabinet Decisions 7
Financial Review 8
"Whistleblowers" 9
Complaints Hearings 9
Security Clearances 10
Effect of Committee Recommendations about Complaints 11
Access to Information and Privacy 11
Canada Evidence Act—I 13
Canada Evidence Act—II 13
The Framework of Accountability 15
Intelligence: Balancing Supply and Demand 16
Foreign Intelligence 18
Release of Information 19
Human Sources 20
Committee Reports and Statements 20

AMENDING THE CSIS ACT

The CSIS Mandate: "Threats to the Security of Canada"

Everything in the *CSIS Act* turns on the definition of "threats to the security of Canada" contained in section 2. During our term, we have become concerned about the scope and the wording of this provision.

Threats to the Security of Canada: paragraph 2(d) (Domestic Subversion)

In testimony to the Justice and Solicitor General Committee on December 17, 1987, the Chairman of SIRC, Ronald G. Atkey, speaking on our behalf, stated that the so-called counter-subversion mandate in paragraph 2(*d*) of the *CSIS Act* applied "regardless of how unlikely [the activities in question] are to lead to violent revolution". He added that "most of the investigations carried out by the [then] counter-subversion branch were authorized either because of the suspected involvement of hostile foreign intelligence services or because of a danger of politically motivated violence". In urging that the Counter-subversion Branch be disbanded, he indicated that the problem was one of proportionality.

With the closing of this branch, and the decision of the Solicitor General that active investigations in the field of counter-subversion would require his personal authorization, we believe that it is now time to urge that this part of the mandate be reassessed. It is our conclusion, in light of the evolving experience with paragraph 2(*d*), that it should now be repealed. Such a repeal would, of course, involve repeal of paragraph 21(5)(*a*), which deals with paragraph 2(*d*) warrants, as a consequence. We realise that there can be a real threat to security posed in any democracy from domestic sources. But we believe that other parts of the mandate offer adequate protection to the security of Canada.

Additionally:

a) The present *CSIS Act* already distinguishes between paragraph 2(*d*) and other aspects of the mandate in providing a maximum time period of 60 days for judicial warrants granted under authority of this provision (paragraph 21(5)(*a*)). Therefore, the *Act* already recognizes that activities under paragraph 2(*d*) require special restrictions.

b) In our 1986–87 Annual Report (page 36), we noted that in counter-subversion, groups are targeted most often under the criteria of undue foreign influence or politically motivated violence. These fears are the concerns of other paragraphs in the section 2 mandate.

c) In 1987, the Solicitor General announced that the Counter-subversion Branch would be disbanded and that any retained files were to be transferred to the operational branches of the Service addressing the concerns noted in paragraph (*b*).

d) We note that last year there were no groups that were subject to investigation solely under paragraph 2(*d*) (1987–88 Annual Report, page 13).

e) The counter-subversion mandate has probably been criticized more than any other provision in the *CSIS Act*.

1. *We recommend*, therefore, that paragraphs 2(*d*) and 21(5)(*a*) be repealed.

Threats to the Security of Canada: paragraph 2(b) (Foreign Influenced Activities)

Paragraph 2(*b*) of the *CSIS Act* defines the following threat to the security of Canada:

> foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person.

Before any activities fall within that definition, certain key characteristics must be present, four in Group A and four in Group B. They must be:

Group A

- foreign influenced;
- within or relating to Canada;
- clandestine *or* deceptive; and
- detrimental to the interests of Canada; or

Group B

- foreign influenced;
- within or relating to Canada;
- detrimental to the interests of Canada; and
- involve a threat to any person.

These requirements are conjunctive: all of them in Group A or Group B must be met before the Service can get involved. A final requirement must also be met, although it is expressed in the negative. As with the threats defined in paragraphs 2(*a*), (*c*), and (*d*), the Service can get involved with any "foreign influenced activities" that include "lawful advocacy, protest, or dissent" only if they are carried on in conjunction with any of the activities referred to in paragraphs (*a*) to (*d*). The key requirements listed above that help define the mandate of the Service are most ambiguous. They are not found in other Canadian legislation, and their use in the *ASIO Act* of Australia has also given rise to considerable controversy. We have had a great deal of experience with the mandate presently contained in paragraph 2(*b*), and we have concluded that it should be revised. The key requirements will be addressed in order.

Foreign Influenced. The phrase "foreign influenced" would cover foreign interest groups, political organizations, individuals, associations and corporations: any such groups or individuals are arguably "foreign" simply because they are not Canadian. The verb "influenced" was used rather than the narrower "directed" employed in the Cabinet Directive defining the mandate of the Security Service of the RCMP.

Within or Relating to Canada. At present, whether the activities are actually carried on in Canada, are directed from Canada, or are conducted or directed outside Canada, they need only be said to be "related" to Canada for the Service to satisfy the second requirement in paragraph 2(*b*). There are no criteria set out in the *Act* to help determine how

much any particular activity must "relate" to Canada before CSIS can take jurisdiction. So long as there is some "reasonable connection" between the activity in question and Canada or its interests, this part of the requirement will be too easily met.

Clandestine or Deceptive. The basic notion of this characteristic relates to secrecy, concealment or threat. The precise meaning of the term "clandestine" is uncertain. It may connote an element of underhandedness or *male fides*, but some dictionary definitions would support an interpretation that merely "secret" activities may be "clandestine". To avoid any uncertainty, we propose that the term "clandestine" be repealed and replaced with a word like "surreptitious", which more clearly connotes some element of underhanded behaviour. The meaning of "deceptive" is clear; it seems to connote dishonesty in the sense that the person who is deceiving knows what he is doing or saying is false or intends to mislead by such falsehood. Where a foreign power "surreptitiously" or "deceptively" intrudes into Canadian national activities, the interference may be every bit as objectionable as espionage. The Service should be amply equipped to address this kind of interference in our national affairs.

Detrimental to the Interests of Canada. The most problematic part of paragraph 2(*b*) is the phrase "detrimental to the interests of Canada". It is not found in any other Canadian enactment. It is almost wholly subjective. no criteria are provided to offer any standard for determining what is "detrimental". Although it is true that Canadian statutes routinely employ such phrases as "the national interest" or "the public interest", such formulations are deliberately used by Parliament when it wishes to confer maximum discretion upon some decision–maker. But this is hardly the kind of broad discretion that Parliament wished to grant to a security service which was required to maintain the principle of a "delicate balance" between the need to acquire information and an individual's right to privacy. The recent national debate on the merits of the Free Trade Agreement illustrates that even well–intentioned, patriotic citizens can differ strongly on what is in "the interests of Canada". We propose that the phrase "detrimental to the interests of Canada" be defined in the *Act*.

Involve a Threat to Any Person. There are fewer difficulties with this phrase, connoting as it does a genuine fear or apprehension of physical or psychological violence. Therefore, we propose only that the term "threat" be modified by an adjective like "serious". This was the step taken by Parliament in response to similar concerns voiced in the context of the mandate contained in paragraph 2(*c*), relating to politically motivated violence.

> 2. *We recommend* that paragraph 2(*b*) of the *CSIS Act* be repealed and replaced by the following:
>
> "foreign directed activities within or directly relating to Canada that are surreptitious or deceptive and that are detrimental to the interests of Canada or involve a serious threat to any person".

Although this formulation of paragraph 2(*b*) is narrower, we believe that it will provide an adequate mandate for the Service. There is no attempt to limit the mandate to interference by "unfriendly nations" only. Nor does this formulation require that the interference occur in Canada—activities occurring in our embassies abroad would be covered, for example, so

long as they are "directly" related to Canada. There is an implicit recognition in the proposal that foreign states may act through ostensible business organizations; consequently, the mandate would not be limited to actions conducted by foreign governments.

"Unwitting" agents of influence, if such agents in fact exist, could not be targeted by the Service under this paragraph. However, foreigners who attempt to "direct" such interference would clearly be subject to CSIS scrutiny. The addition of the modifier "serious" to threat is designed to limit the definition while still recognizing that the threat could occur either in Canada or abroad (such as a threat to a relative in one's homeland).

We believe most emphatically that the phrase "lawful advocacy, protest or dissent" must continue to limit this aspect of the Service's mandate as well as the entire definition of "threats to the security of Canada".

3. *We also recommend* that as precise a definition as possible of "detrimental to the interests of Canada" be included in the amended *CSIS Act*.

Drafting legal definitions is an arcane art and so we will not attempt to suggest a precise definition of the phrase "detrimental to the interests of Canada". We will, however, offer wording which could form the basis for discussion by individuals representing all points of view during the forthcoming Parliamentary hearings, as follows:

"detrimental to the interests of Canada" means activities which are foreign directed, are surreptitious or deceptive, and are directed toward:

a) diminishing the sovereignty or territorial integrity of Canada,

b) weakening Canada's military defences,

c) harming Canada's international relations with any nation or organization,

d) seriously endangering the lives, health or safety of Canadians,

e) obtaining, illegally, or without proper authorization, any information or thing classified in the national interest by the Government of Canada, or

f) the bribery, coercion, or corruption of Canadians in respect of activities falling within paragraphs *a*), *b*), *c*), *d*) or *e*).

Overcoming Isolation

We note that the Independent Advisory Team which investigated the Service in 1987 (the Osbaldeston Committee) recommended that "the career paths of CSIS staff should provide for movement within both the security intelligence community and the public service" (page 17).

We believe that the Service's Analysis and Production Branch in particular would profit considerably if public servants from elsewhere in government, academics, or others with special expertise, could work with it. CSIS officers engaged in analysis and assessment also benefit by their ability to work in related agencies of government or universities.

Although we recognize that there would be a cost incurred in acquiring the extensive security clearances required by those who would rotate through the Service, we believe that the

benefits would far outweigh the costs. CSIS believes that it already has the capacity to institute staff exchanges with the public service.

> 4. However, for greater certainty, *we recommend* that the *CSIS Act* be amended specifically to provide for the rotations by public servants and others with special qualifications through CSIS, subject to provisions that would safeguard the identity of employees engaged in the covert operational activities of the Service.

Grievance Procedures

Under the *CSIS Act*, SIRC cannot deal with complaints that are subject to grievance procedures set out in the *CSIS Act* or the *Public Service Staff Relations Act*. The *CSIS Act* contemplates that grievances might be adjudicated by members of the Public Service Staff Relations Board (PSSRB). In some cases, for example those involving salary matters and the like, SIRC would have little interest or particular competence in a dispute before the PSSRB. However, in many other situations, SIRC might be vitally interested. For example, a grievance involving alleged insubordination could arise if a member of the Service were to disagree strongly with how the Service was complying with a ministerial direction in a sensitive area.

> 5. Therefore, *we recommend* that CSIS be required to give timely notice to SIRC in advance of all grievance hearings that are conducted pursuant to subsection 8(3) of the *CSIS Act*.

SIRC should be entitled to be briefed in advance by the Service and to attend any grievance hearing. In this way, SIRC may better determine whether issues arising in a labour relations context merit independent investigation in the discharge of SIRC's separate responsibilities.

Warrants

The *CSIS Act* does not give SIRC any specific authority with respect to warrants. However, we have reported on warrants pursuant to our general duty to ensure that there is no "unreasonable or unnecessary use by the Service of any of its powers" (section 40) and our responsibility to "compile and analyze statistics on the operational activities of the Service" (subparagraph 38(*a*)(vii)).

In testimony to the Justice and Solicitor General Committee on November 20, 1986, Mr. Atkey discussed the fact that there was less statistical information concerning warrants available under the *CSIS Act* than had been available under the *Official Secrets Act*. He indicated his belief that parliamentarians are entitled to more of such information. Another member of the Committee, Jean Jacques Blais, noted that since it was the role of the Committee to review warrant affidavits and their concordance with the materials upon which they were based, SIRC will be in a position, eventually, to give broad assurances to Canadians that the *Act* is being followed. In our three most recent Annual Reports (1985–86, page 18–19; 1986–87, page 11, and 1987–88, pages 19 and 59) we have expressed our concerns about this matter.

Under the *Official Secrets Act*, generally, each warrant authorized only one covert technique against only one target, whereas one warrant under the *CSIS Act* can authorize the use of many powers against many targets. We do not think that aggregate warrant statistics under the present legislation are very helpful. Serious concerns about Canadians' privacy rights under the *Canadian Charter of Rights and Freedoms* prompt the following recommendation.

6. *We recommend* that the *Act* be amended to provide specifically that SIRC have the responsibility to compile and analyze warrant statistics and that SIRC be required to publish annually statistics containing the number of Canadian citizens or landed immigrants who have been affected by surveillance powers granted to the Service under judicial warrants.

We have often raised the issue of emergency warrants (1985–86 Annual Report, page 44; 1986–87 Annual Report, page 12; 1987–88 Annual Report, page 57). The elaborate procedures for obtaining a warrant that are currently in place offer important safeguards. But we are concerned that it might take too long in an emergency to obtain a warrant if the regular procedures are followed. Under the *Official Secrets Act*, warrants could be obtained within about three hours.

7. *We recommend* that section 21 of the *CSIS Act* be amended so as to permit the Director of the Service, with the agreement of the Solicitor General in each case, to issue a short–term, non–renewable warrant that would require an application to the Federal Court within 96 hours. There should also be the stipulation that SIRC must be notified within one week of the application.

Still in the area of warrants, we have also raised the issue of solicitor–client communications (1986–87 Annual Report, pages 19-20; 1987–88 Annual Report, page 58). Such communications are being protected by warrant conditions prohibiting interception of communications at the office or residence of the lawyer, or at any other place normally used by the lawyer to consult with clients. Furthermore, the interception of calls between a target and his or her lawyer are limited to calls that the Director or a regional director general have determined relate to the threat specified in the warrant.

We are pleased that such conditions are routinely included in warrants, but would prefer that such safeguards be enshrined in legislation. The *Criminal Code*, for example, explicitly protects solicitor-client communications. Of course, we recognize that terrorists or other groups whose activities constitute threats to the security of Canada may include lawyers in their number. Our concern is limited to communications with lawyers that fall clearly within the solicitor-client description. Our proposals would pertain solely to lawyers who are acting in their capacity as legal counsel.

8. *We recommend* that a section be added to Part II of the *CSIS Act* to provide statutory protection to solicitor–client communications.

9. Further, *we recommend* that another section be added to Part II of the *CSIS Act* listing warrant limitations that shall be considered by Federal Court judges.

Devil's Advocate (Amicus Curiae)

Since 1987, a Department of Justice lawyer, responsible to the Deputy Solicitor General, has appeared at the Warrant Review Committee as "devil's advocate".* But this official is exercising a more limited mandate than we intended when we first proposed a devil's advocate, in our 1986-87 Annual Report (page 9).

At present, the devil's advocate does no more than ensure that the information CSIS intends to cite in a warrant application is accurate. We had in mind, rather, someone who would challenge the need for a warrant at all—someone to make the case that the proposed target (who does not, of course, even know a warrant is being sought) might make.

We are also concerned about the location of the devil's advocate's intervention in the process. Sitting on the Service's internal Warrant Review Committee, the devil's advocate can too easily be perceived as a mere token at best, an insider at worst. We believe that the devil's advocate should appear before the Federal Court itself.

Therefore, although the warrant application system seems to be working much better than before, we believe that considerations involving the appearance as well as the substance of natural justice prompt reform in this context.

10. *We recommend* that Part II of the *CSIS Act* be amended to add a section requiring that a "devil's advocate", appointed by the Court, appear at each Federal Court hearing at which a judicial warrant is sought.

11. *We further recommend* that where possible this lawyer not be a government lawyer, but be drawn from a list of security-cleared outside counsel.

For example, SIRC has a roster of such lawyers. To avoid any conflicts of interest, these lawyers could be appointed in alphabetical order or on some other random basis. The total number of new warrants and renewed warrants each year has fallen significantly, so this practice would not appear to represent a serious drain on resources.

Cabinet Decisions

Our current inability to see Cabinet decisions that affect CSIS has proved to be a problem in one instance we know of. During 1988-89, we were refused access to the Service's Multi-Year Operational Plan (MYOP) because it is prepared for submission to Treasury Board, a committee of Cabinet. In this instance, a compromise was reached: while the MYOP document itself was withheld, we were given the information it contains.

We have received assurances from the Ministry of the Solicitor General that cabinet decisions will be re-written and passed to CSIS as ministerial direction, which we automatically receive pursuant to subsection 6(2) of the *CSIS Act*. However, we have no way of

* By devil's advocate we mean an official appointed to argue a point of view, with which he or she may or may not personally agree, for the purpose of ensuring that all aspects of a matter are fully considered.

knowing whether this procedure is foolproof or whether future Solicitors General would agree to continue the practice.

As we stated in our 1987-88 Annual Report, those of us who have been members of cabinets cannot understand why the statute would preclude the Committee from seeing cabinet decisions relating to CSIS operations. In our view, current arrangements create unnecessary public suspicion.

We recognize, of course, that we should not have access to records which would reveal the cabinet's decision making process. However, cabinet decisions are the executive authority used by all departments and agencies to justify their activities. It is essential that SIRC have access to cabinet documents directed or related to CSIS if it is to be in a position to review CSIS' performance of its duties and functions. Therefore, we believe that any cabinet decisions in CSIS' possession which relate to its duties, functions, or resources should be available to the Committee. Similarly, any memoranda to cabinet prepared by or about the Service should be available. Obviously, members of the Review Committee would be enjoined from revealing the content of confidences of cabinet to third parties; they are Privy Councillors and are bound by the same oath as are all past and present members of cabinet.

> 12. *We recommend* that subsection 39(3) of the *CSIS Act* be repealed, thereby permitting the Security Intelligence Review Committee to have access to all information under the control of the Service, regardless of its source.

Parliament might also consider amending subsection 31(2) so as to allow the Inspector General access to all information under the control of the Service, including confidences of cabinet.

Financial Review

In the past, the Auditor General audited the Security Service of the RCMP and, since he has a responsibility to verify how all money derived from the Consolidated Revenue Fund is spent, he has a statutory duty to audit CSIS as well. His auditors all have the requisite degree of security clearance to do the job. Now that the recommendations of the Osbaldeston Committee have been implemented, we think that it would be timely for a system audit of the Service to be conducted. We think it highly desirable for the Committee to have an element of responsibility for such an audit, given its understanding of the operational aspects of the Service's mandate.

Under section 38 of the *CSIS Act*, no specific authority is conferred upon SIRC to assess the Service's financial performance; however, the Committee may "review generally the performance by the Service of its duties and functions". The Committee believes that this power is technically sufficient to enable it to assess the Service's financial management.

> 13. Nevertheless, and out of an abundance of caution, *we recommend* that a subparagraph be added to section 38 of the *Act* to indicate clearly that the Security Intelligence Review Committee has the authority to undertake financial reviews of the Service in cooperation with the Auditor General.

"Whistleblowers"

Many governments have recently attempted to remove potential obstacles to public officials who wish to expose activities that they think are wrong. There is a so–called "Whistleblowers' Protection Act" in the United States (*Civil Service Reform Act*, 1978, 5 U.S.C. s.7701 *et seq.*). Similar reform is proposed in Ontario, and protection for "whistleblowers" is found in such recent federal legislation as the *Canadian Environmental Protection Act* (s.58(4) of that *Act*, being S.C. 1988, c.22). As we noted in our 1987–88 Annual Report (page 59), in the United Kingdom, a special official takes "leaks" from members of MI5, who are not required to identify themselves.

Under the *CSIS Act*, there is no protection from disciplinary measures provided to employees of the Service who expose perceived wrongdoing to the Committee. Indeed, complainants must first make their concerns known to the Director, who may be precisely the person that the employee wishes to avoid.

> 14. Accordingly, *we recommend* that the *CSIS Act* be amended by adding subsection (3) to section 41 to guarantee anonymity to CSIS employees who complain to SIRC, and to guarantee that if such complainants are eventually identified, they will not face any disciplinary measures solely by reason of making such complaints.

Complaints Hearings

Under the *CSIS Act*, SIRC hearings must be conducted in private. Under subsection 48(2) of the *Act*, no one is entitled as of right to be present when representations are made to the Committee by any other person. In 1985, the Committee adopted quite elaborate rules of procedure in relation to the investigation of complaints made to it. Separate procedures have been prepared for complaints involving the denial of security clearances in employment, and in immigration and citizenship matters. These procedures were adopted by the Committee pursuant to its right to do so under subsection 39(1) of the *Act*. The extensive procedural safeguards that the Committee has generated and distributed to the public are in marked contrast to the often abbreviated process that applies, for example, before a deputy head of a government institution reaches a decision to deny a security clearance. SIRC's investigations typically are very extensive and the hearing that is often held usually resembles a formal adjudication held by an administrative tribunal exercising quasi–judicial powers.

When public knowledge of evidence about to be adduced might be injurious to national security, perhaps because it would reveal sources or otherwise constitute a "threat to the security of Canada", complainants and their counsel are excluded while the evidence is heard by the Committee. There have been several challenges initiated in the Federal Court questioning the Committee's procedures in hearing complaints. So far, none of these challenges has succeeded and SIRC's rules of procedures and underlying practices have "passed muster" when measured against the *Charter of Rights and Freedoms* and the requirements of procedural fairness. Obviously, SIRC must abide by the outcome of any litigation that is not yet completed.

In oral hearings, it is in the discretion of the member hearing the case to determine whether or not a party should be excluded while testimony is given by another party.

SIRC has evolved a procedure by which the counsel and the excluded party (usually the complainant) are then brought back into the room and given the gist of the evidence, without disclosing the national security information. They are then allowed to ask questions, and, where possible, cross-examine, on the basis of this summary.

We believe that the role now played by counsel to the Committee under our rules of procedure has proven to be quite fair and effective in this context. During complaint hearings when parties are excluded, Committee counsel is specifically instructed to ask Service witnesses the kinds of questions that one would expect the complainant's counsel to ask and to cross-examine with equal vigour. The summary of evidence that is later provided to the excluded party is usually negotiated by counsel for CSIS and SIRC under the supervision of the presiding member. What flows to complainants and their counsel is sufficient information to enable them to be as fully informed as possible of the case against them.

Only one problem has arisen with the present wording of the *Act* respecting investigations. Subsection 48(2) states:

> 48(2) In the course of an investigation of a complaint under this Part by the Review Committee, the complainant, deputy head concerned and the Director shall be given an opportunity to make representations to the Review Committee, to present evidence and to be heard personally or by counsel, but no one is entitled as of right to be present during, to have access to or to comment on representations made to the Review Committee by any other person.

It has been asserted that since the subsection can be read as denying access to "representations" only, it does not deny access to the presentation of evidence or the personal appearance by any other person. Such an interpretation, if upheld by the courts, would make Committee investigations dealing with classified national security matters all but impossible.

We do not believe that this assertion is well-founded. However, it would be useful to reword subsection 48(2) to clarify its intent.

> 15. *We recommend*, therefore, that the words "evidence adduced, or statements made" be added to subsection 48(2) so that it provides:
>
> ... but no one is entitled as of right to be present during, to have access to or to comment on representations made, evidence adduced, or statements made to the Review Committee by any other person.

Security Clearances

Without a security clearance, many employment opportunities—both in the public and private sectors—are effectively lost. The *CSIS Act* allows only some affected persons to complain to the Committee (s. 42).

First, the person must have been denied employment, dismissed, demoted or transferred, or denied a promotion or a transfer in government or else be refused a contract to supply goods and services to government for the same reason. As we noted in our 1987–88 Annual Report (page 56), the present wording means that when a person is fired or not

hired by a contractor in order to remove an obstacle to doing business with government, he or she has no effective redress. In addition, where certain activities require the use of federal facilities, such as airports, which are denied to individuals lacking a security clearance, some persons will be unemployable. They too have no right to complain to the Committee.

Second, the decision to deny a security clearance must be one taken by a "deputy head".

Third, the right to complain at all is predicated upon a denial. This term may be narrowly interpreted to mean that only an outright refusal will trigger the statutory right. What happens if the authorities delay unreasonably, but never get around to a formal denial? At present, the individual concerned can complain to the Review Committee pursuant to the procedures specified in section 41, but more protection against such delay may be needed in the *Act*.

Fourth, the *Act* refers to a loss of employment opportunity "by reason *only* of the denial of a security clearance". What happens if the employer can honestly say that there were other reasons, albeit very secondary ones? This particular point has been cited on at least two occasions in challenges to the Committee's jurisdiction to investigate a complaint.

We believe that the right to complain to the Review Committee should be available to anyone who is denied a security clearance. There should not be categories of Canadians or landed immigrants who do not have the right to complain to SIRC when they are denied a security clearance, while others have the right to a full investigation by the Committee. It is a fact of life in the modern world that the denial of a security clearance usually has an immediate effect on an individual's employment; it always has a long term effect on the individual's employment potential.

In any event, above and beyond the serious effects on employment, no Canadian or landed immigrant should be put in the position of having his or her loyalty questioned to such an extent that a security clearance is refused without having an automatic right to request an investigation by the Review Committee.

Often, individuals are denied *any* level of security clearance, but in some circumstances individuals who require a TOP SECRET clearance for their employment are granted only a SECRET or CONFIDENTIAL level of security clearance. This usually has the same effect on the individual's employment as an outright denial of any level of security clearance would have had.

The amendments we propose would provide the right to an investigation by the Review Committee to any Canadian or landed immigrant denied a security clearance at the level required.

16. *We recommend* that subsections 42(1) and (2) be repealed and replaced by:

"42(1) When a security clearance, required by the Government of Canada for an individual for any purpose, is denied or is granted at a lower level than that required or is downgraded to a lower level than that required, the deputy head or other person making that decision shall send, within ten days after the decision is made, a notice informing the individual of the denial of a security clearance at the required level, and

of the individual's right under this section to complain to the Security Intelligence Review Committee."

The remainder of section 42 would require minor consequential amendments.

Effect of Committee Recommendations about Complaints

At present, the Thomson case is again before the Federal Court of Canada. There is a disagreement between the Appeal and Trial Divisions of that Court as to whether the Committee's recommendations on security clearances should be binding upon deputy heads. Regardless of the eventual outcome of this case, Parliament may wish to clarify its intent during the five-year review of the *CSIS Act*.

We note that in Australia's *ASIO Act*, the "findings" of the Security Appeals Tribunal must be treated as "superseding" the original security clearance (s. 61).

We believe that it would in no way violate conventions of ministerial responsibility if Parliament decided to empower the Security Intelligence Review Committee to make final determinations in those cases where it disagrees with a decision of a deputy head to deny a security clearance. Decisions that determine whether an individual may work in a chosen field directly affect the rights of individuals. To be vindicated before a neutral tribunal like SIRC, only to learn later that a security clearance has still been denied by a deputy head in his or her absolute discretion must be deeply disturbing.

Finally, the new Government Security Policy (GSP) of June, 1986, specifies that the Security Intelligence Review Committee constitutes the redress procedure for all public servants who are denied a security clearance. We believe that the clear implication of these arrangements is that SIRC has decision-making powers.

17. Therefore, *we recommend* that subsection 52(2) of the *Act* be amended to provide that Committee rulings in respect of security clearances are final and binding upon a deputy head.

Access to Information and Privacy

In the normal course of events, the powers of the Security Intelligence Review Committee will almost certainly overlap with the separate powers exercised by the Information Commissioner or the Privacy Commissioner. This has already occurred with respect to the Privacy Commissioner.

In investigating complaints under the *Access to Information Act* or the *Privacy Act*, either Commissioner may have entered into negotiations with the Service, perhaps with respect to the same records that the Committee wishes to inspect in the discharge of its separate statutory responsibilities. The Committee believes that access by either Commissioner should not be hampered because of a parallel SIRC investigation or vice versa. Each independent agency has its own statutory responsibility to discharge. Though we believe that the present wording of the *Act* amply provides for SIRC access under any and all circumstances, some government authorities are not entirely convinced of this.

18. Therefore, *we recommend* that Parliament consider the advisability of clarifying this issue by adding a paragraph to subsection 39(2) of the *CSIS Act* specifying that the Committee is entitled to have access to any information under the control of the Service, notwithstanding the existence of any investigations that may be undertaken by the Information Commissioner or Privacy Commissioner.

The Canada Evidence Act—I

In testimony to the Justice and Solicitor General Committee on November 20, 1986, the Chairman replied to a question regarding section 37 of the *Canada Evidence Act*. Under this section, a member of CSIS can curtail testimony in criminal trials. This practice has been much criticized and Mr. Atkey reported that "there is discomfort within the Service with the particular wording and operation of that section... I think this is a problem area" (page 2:16). He then suggested that this was a good topic for consideration during the parliamentary review of the *CSIS Act*. He agreed that it was "a terribly awkward procedure... [and that there was] a potential for prejudice to the accused in a criminal trial". However, SIRC fully appreciates why any security intelligence service would struggle to keep its sources and "tradecraft" secret. We agree that CSIS intelligence should only rarely be used as evidence in court proceedings. However, it must be recognized that there will be exceptions and procedures should be available to protect the national interest when that happens.

In our 1986–87 Annual Report (page 25–26), we noted that in section 486 of the *Criminal Code*, the public may be excluded from courtrooms for various reasons that are listed.

19. In that light, *we recommend* that section 486 of the *Criminal Code* be amended

a) to add the phrase "threats to the security of Canada, as defined in section 2 of the *CSIS Act*" so that the judge would have the power to exclude the public from portions of trials where national security matters might foreseeably be raised; and

b) to allow a judge to exclude the defendant and counsel as well as the public when security matters were raised.

The Canada Evidence Act—II

Until the enactment of amendments to the *Canada Evidence Act* in the early eighties, the Solicitor General could sign a certificate to the effect that the disclosure of certain information would be injurious to national security. The minister's certificate was final and completely unassailable before any court.

Section 38 now provides a means by which the written or oral objections to evidence on national security grounds may be reviewed. The review may be carried out by the Chief Justice of the Federal Court or by a judge designated by him or her. In other words, the review of the evidence in question can only be carried out by one specified person or the nominee of that person, and the hearing must be carried out *in camera* and in the National Capital Region.

This process was designed to enhance the rights of individuals involved in criminal cases before the courts. However, these rules have caused problems in certain situations arising after the Review Committee was created in July, 1984.

Review Committee recommendations/decisions are sometimes challenged before the Federal Court of Appeal under section 28 of the *Federal Court Act*. When this occurs, special direction must be obtained from the Court to protect national security documents which would normally be made public if the usual rules were followed. In addition, when the Department of Justice objects to the disclosure of national security information to the appellant, the Court must then await a ruling from a judge designated by the Chief Justice as to the validity of the "national security" objection. This ruling by the designated justice can be appealed to the Federal Court of Appeal, and Appeal Court justices can then examine the documents in question. Ironically, however, without an appeal in the face of a ruling in favour of the Crown by the designated judge, the Appeal Court cannot examine the documents.

This complex process takes place as part of a procedure whose purpose is to review the Review Committee's recommendation/decision following an investigation. Such an investigation by the Review Committee examines all documents, whatever their classification, and hears oral evidence regardless of its "national security" sensitivity. All classified evidence is withheld from the complainant during a Review Committee investigation.

Since the Review Committee's recommendation/decision is very often based, for the most part, on "national security" evidence, any court charged with reviewing the Review Committee's conclusions and procedures could only do so effectively if it also had access to all the evidence considered by the Review Committee.

20. Accordingly, *we recommend* that the *CSIS Act* be amended to provide, in the event of judicial review, that the Federal Court of Appeal have exclusive jurisdiction under s. 28 of the *Federal Court Act*, and be entitled to review any Review Committee report rendered pursuant to section 42 or any report affecting the rights of an individual rendered pursuant to section 41, together with all relevant documents.

21. *We further recommend* that special procedures be authorized either by statute or by regulations to enable Review Committee files and documents to be transferred to the Federal Court of Appeal without the nature of those documents being made public, and, where necessary, without even the existence or absence of such files being acknowledged.

Acceptance of these recommendations would have the beneficial side-effect of eliminating any requirement for an individual to challenge a Review Committee ruling under section 18 of the *Federal Court Act*. This procedure is unfair at present because the individual concerned usually knows very little indeed of the case made against him and has very little chance of being able to construct an adequate application for judicial review. The practical effect of the present procedure is to deprive most individuals who complain under section 41 of the *CSIS Act* of the right to challenge a Review Committee report effectively.

The Framework of Accountability

After five years of experience, the Committee has formed strong opinions on whether the institutions now set out in the *Act* are effective and necessary. In our unique Canadian model, the Solicitor General, accountable to Parliament, is ultimately responsible for the Service. Under the *Act*, there is also a full–time "insider" in the Inspector General, who is "the Minister's person" and assists him in carrying out his responsibility for CSIS. SIRC completes the picture. It is a part–time, tri–partisan committee, independent of the government of the day. In our view, the combination of a tri–partisan group of part–time Privy Councillors found in SIRC has worked well. Consensus has usually been achieved and partisanship has been minimized. Another advantage is that as compared to the experience with oversight bodies elsewhere, "leaks" have not been a problem.

22. *We recommend* that the *CSIS Act* retain the Security Intelligence Review Committee with its present jurisdiction.

The alternative, of course, is to provide for a standing committee of Parliament to oversee CSIS. There are two such committees in the Congress of the United States. In Australia, Parliamentarians were recently appointed to the Parliamentary Joint Committee on the Australian Security Intelligence Organization; however that Committee is somewhat limited in gaining complete access to documents held by ASIO. Moreover, the McDonald Commission recommended a joint parliamentary oversight committee. Nevertheless, we think that the experiment with SIRC has proven successful and propose that the Committee be retained in a revamped *CSIS Act* as the principal oversight body. In urging this continued role for SIRC, we would make a related recommendation.

23. *We recommend* that the *CSIS Act* contain a provision requiring the Director of the Service to offer to consult regularly with the leaders of the major opposition parties represented in Parliament, in order to keep them informed on matters relating to security.

This kind of provision is found in the *ASIO Act* (s.21) and, to our knowledge, has worked well. It would strengthen the role of Parliament in the chain of accountability.

Should SIRC be empowered to review the activities of all the other institutions that comprise the Canadian intelligence community? In Appendix C of our 1987–88 Annual Report, we outlined the main constituents of Canada's intelligence network. In testimony to the Justice and Solicitor General Committee on June 3, 1986, Mr. Atkey stated that "this was an issue that Parliament should address at some time" (page 21:25). Mr. Atkey did not discuss whether such expanded oversight duties should be conferred upon SIRC.

Australian legislation provides for an independent oversight body for the entire Australian security intelligence community. The Office of the Inspector General of Intelligence and Security is responsible for "oversight and review of the compliance with the law by, and the propriety of particular activities of, Australian intelligence or security agencies" (*The Inspector General of Intelligence and Security Act*, 1986, section 4). This Office oversees the Australian counterparts to CSIS, the Communications Security Establishment, the Office of National Assessments, and the directorates of intelligence and security in the Department of National Defence, as well as ASIS, Australia's counterpart to the CIA.

In the United States, of course, the situation is similar to that in Australia: all intelligence agencies are subject to review and oversight by Congressional committees.

The McDonald Commission recommended that the review body it proposed should cover all federal agencies engaged in the clandestine collection of intelligence, except for the RCMP. (Recently, the RCMP admitted to the formation of a National Security Investigation Section (NSIS). There seems to be no obvious reason why this organization should not also be subject to external review.) Its report suggested that unless the review body was given this broader jurisdiction, "it would be all too easy for a government to evade its scrutiny by *de facto* transfers of responsibilities from the security intelligence agency to some other organization which is not subject to its review" (McDonald Commission Report, Volume 2, page 885).

We observe that there is still no review mechanism in place for the balance of the Canadian intelligence community apart from ministerial responsibility. Of course, if Parliament were to accept our recommendation to establish an Intelligence Assessment Office (see page 18), all Canadian intelligence agencies would benefit from the resulting "quality control" which would be exercised by such a body. But such quality control would not be the equivalent of a system of review. We believe that it would be appropriate for Canada to follow the Australian and American practice by instituting, in line with the McDonald Commission's recommendations, a system of review for all federal agencies engaged in the collection of intelligence.

24. *We recommend* that Parliament consider enacting legislation to provide for the independent monitoring of other institutions within Canada's intelligence network.

We have no strong view as to whether this responsibility could be assumed by an expanded SIRC or some other independent body established for this purpose.

Intelligence: Balancing Supply and Demand

Especially at a time when sound financial management is at the forefront of the public's attention, Parliamentarians will be particularly interested in assessing the cost–effectiveness of the Service. As an intelligence agency, is CSIS gathering and analyzing information effectively and then transforming it into usefu. "intelligence"? SIRC defines "security intelligence" as "the collection, from both open and covert sources, and analysis of information which provides advance warning and advice about activities which may constitute a threat to the security of Canada".

There are two major categories of intelligence: security intelligence which can originate at home or abroad but which deals with threats to the security of Canada, and foreign intelligence which deals with information about other countries. The Service is the primary contributor of the former.

A further useful distinction between different types of intelligence was made by the Independent Advisory Team that investigated the Service in 1987 (the Osbaldeston Committee). *Operational intelligence* is "related to the investigation of particular activities considered threatening to the security of Canada". It relies heavily (but not exclusively) on investigative techniques, is usually short–term and is produced for specific consumers or

for a specific purpose. *Strategic intelligence* "relies more heavily on research using information from all sources, tends to be longer term and more global in scope and is produced for an interdepartmental audience or for the government as an entity". It is "evaluated in the context of other Canadian national interests".

In our 1987–88 Annual Report, we summarized the results of our investigation of the Analysis and Production Branch in CSIS. We concluded that significant improvements have been made. However, we noted a lack of the multi-disciplinary input necessary in generating the economic, political and social components of comprehensive strategic intelligence. For instance, to date there has been little input from specialists external to government. In our view, changes in the environment of the Branch are still required if CSIS is to move away from producing mainly operational intelligence.

We note that the Osbaldeston Committee was also concerned about the intelligence produced by CSIS and "the lack of a coordinated system for production". Similarly, in 1987 the Senate Special Committee on Terrorism and Public Safety (the Kelly Committee) recommended that "the Security and Intelligence Secretariat of the Privy Council Office be expanded and strengthened to provide a single focus for the gathering of intelligence and assessments from federal departments and agencies for review by the Intelligence Advisory Committee (IAC) and for dissemination to the relevant federal departments and agencies" (page 61).

The IAC is "the closest Canada comes to having a single focus for the gathering, analysis, discussion and dissemination of defence and security information and intelligence". IAC members cooperate and coordinate the production of intelligence, drawing on research and analysis carried out by federal agencies, notably CSIS, the Department of External Affairs (DEA), the Department of National Defence (DND) and the Communications Security Establishment (CSE). At present, the IAC serves all departments; it also supports the Cabinet Committee on Security and Intelligence which is the Prime Minister's vehicle for exercising leadership and setting priorities for both the security intelligence and foreign intelligence agencies.

The McDonald Commission also urged that there be a centralized assessment function in Canada, with a centralized assessments body. It recommended that a Bureau of Intelligence Assessments be established in the Privy Council Office (Second Report, volume 2, at pages 854–56). The Bureau would have no collection capacity. The McDonald Commission urged that the Bureau be separate from the Security and Intelligence Secretariat, with a nucleus of its own intelligence analysts augmented by officers seconded from the departments and agencies of government with responsibilities for security and intelligence matters. The Director General of the Bureau would report to the Prime Minister through the Secretary to the Cabinet and would also be a member of the Intelligence Advisory Committee.

The Commission also urged, however, that the security intelligence agency (now CSIS) should have a strong analytic capacity, producing both short-term and long-term threat assessments. Its assessments would be used by the proposed Bureau, and its intelligence officers would frequently be part of groups working under the auspices of the Bureau to produce long-term estimates and priorities.

We have been favourably impressed with Australia's Office of National Assessments (ONA). In Australia, a clear distinction is made between "collection agencies" and "assessment agencies". Established over ten years ago, the ONA is responsible for collating and evaluating information on many political, economic and strategic matters. The Director-General of the ONA reports to the Prime Minister. It does not collect intelligence as such; instead, it assesses what the collection agencies in that country's security intelligence community—including the Australian Security Intelligence Organization (ASIO)—may provide to it. The ONA also produces reports on specific issues to assist ministers in formulating policy. It was created as an independent body designed to give objective, unfettered advice. It also assists the government in setting its intelligence priorities and requests the collection agencies to obtain specific information it lacks. The ONA consists of a mix of analysts drawn from both the public service and the private sector, including academics with expertise in specific areas. The previous head of the ONA, Michael Cook, was recently appointed Australian ambassador to Washington. He has been replaced by Australia's ambassador to Japan.

25. *We recommend* that Parliament examine the feasibility and merits of establishing an institution similar to Australia's Office of National Assessments.

Such an Intelligence Assessment Office would assess the intelligence product generated by the Service, as well as by other federal agencies, such as CSE and the Foreign Intelligence Bureau in DEA. In addition, it would assist the Cabinet Committee on Security and Intelligence in setting the Government's priorities, and would exercise a quality control function over the intelligence produced by all federal agencies. Like CSIS, it might be given a statutory mandate; like ONA, it should encourage the involvement of a mix of qualified citizens, including experts from outside the government. It would report to the Intelligence Advisory Committee.

Foreign Intelligence

In modern times, Canada has not had a secret foreign service. Should we have an offensive intelligence-gathering function, like the CIA in the United States or the Australian Secret Intelligence Service (ASIS)? Since we have no capacity to collect foreign intelligence by covert human means, we are dependent upon other countries for some types of information about foreign countries, which may pose a threat to Canadian independence in some circumstances. To the extent that covert sources of intelligence are an asset in gaining access to markets and technologies and in international bargaining, Canada will be at a disadvantage with its major trading partners. However, it is by no means clear that Canada needs a secret foreign service.

In light of its location and the difficulties it had in obtaining the foreign intelligence it needed from its allies, Australia established ASIS to concentrate on areas of particular interest to that country. Both political and economic intelligence is generated for Australian policy-makers. There does not appear to be any comparable need in Canada for an "offensive" foreign intelligence agency. However, the case may be more compelling for security intelligence and perhaps criminal intelligence relevant to Canada that is collected abroad.

The Committee is opposed to the establishment of a separate, offensive foreign intelligence agency for Canada. We simply do not believe that the case has been made for such an agency. However, we believe that the *CSIS Act* could provide at least the possibility of the collection of foreign intelligence by CSIS, should the need arise.

> 26. Therefore, *we recommend* that section 16 of the *Act* be amended to remove the words "within Canada".

This amendment would enable CSIS to assist the Minister of National Defence or the Secretary of State for External Affairs in collecting intelligence relating to the capabilities, intentions or activities of foreign states or persons from any source whatsoever. Under the section, CSIS would only be able to assist outside Canada if it received a "personal request in writing" from either Minister and obtained the written consent of the Solicitor General as well. Such an amendment should not impair the ability of SIRC to review the operations of the Service, either at home or abroad.

However, in the event that Parliament chooses to make this amendment to section 16 of the *Act* and there is any doubt as to SIRC's jurisdiction in this regard, we would propose that an amendment be made to section 38.

> 27. *We recommend* that section 38 of the *Act* be amended to clarify the Committee's authority to monitor any CSIS operations that may take place outside Canada.

The adoption of recommendations 26 and 27 would not necessarily mean that there would be any real change in CSIS operations. However, in considering such an amendment, Parliament could debate whether it wanted to provide the opportunity for CSIS, in particular cases.

Release of Information

Section 19 of the *Act* limits the disclosure by CSIS of information it has collected, using its extensive powers. We believe that in the spirit of the *Act* the same limitations apply to disclosure of such information by the Solicitor General and by officials and exempt staff in the Ministry of the Solicitor General; they have access to secret CSIS information, and uncontrolled disclosure by them would make a mockery of the carefully drafted protections found in section 19. However, although we have no reason to believe there has been any impropriety, we have learned that the Solicitor General and his officials and staff do not believe they are bound by this section.

> 28. *We recommend*, therefore, that the limits prescribed by section 19 of the *CSIS Act* apply equally to the Solicitor General and to all officials and exempt staff in the Ministry of the Solicitor General having access to information obtained by CSIS in the performance of its duties and functions.

In another respect, however, we believe the disclosure provision should be broader. Section 19 now makes provision for disclosure to a "person in the public service of Canada" under some circumstances. By a narrow reading, this could mean only paid officials employed under the terms of the *Public Service Employment Act*. We believe it should also include Senators and Members of the House of Commons.

29. *We accordingly recommend* that paragraph 19(2)(*d*) of the *CSIS Act* be amended to permit disclosures to Senators and MPs on the same basis as to Ministers of the Crown and a "person in the public service of Canada".

Human Sources

As has been stated by the McDonald Commission and by this Committee, the most intrusive investigative tool is probably the "human source". A "human source" is a person who informs the Service of the activities of a CSIS target. The human source may have been recruited when he or she was already in a position close to the CSIS target, or may have been asked to gain such a position by infiltrating the target's organization or circle of friends. Human sources are usually paid according to the value of the information they provide. Some have suggested that the use of human sources be allowed only under the authority granted by a judicial warrant, in the same way as other intrusive techniques are presently authorized. We believe that this would put too onerous a restriction on the Service, and would, in many circumstances, be most difficult to implement in a practical way. It would be difficult, for example, to fit casual or "walk-in" sources, sources under development, and many unpaid sources into such a scheme.

However, we believe that the Service should be required to observe strict ministerial guidelines in the use of human sources.

30. *We recommend*, therefore, that the *CSIS Act* be amended to prescribe that the Solicitor General may issue precise guidelines to the Service on the use of human sources. Such guidelines would be passed to the Review Committee automatically pursuant to subsection 6(2) of the *Act*.

Committee Reports and Statements

Section 55 of the *CSIS Act* provides for consultation between the Review Committee and the Director when SIRC is preparing certain reports, so as to ensure compliance with the security requirements set out in section 37 of the *Act*. Though we believe the intent of the section is clear, it does not state that, in case of disagreement, the final decision as to what may be included in a report or statement is that of the Review Committee.

31. *We recommend*, therefore, that:

(a) the opening words of section 55 be amended to provide that before determining the content of a statement or report described in section 55, the Review Committee shall consult with the Director in order to ensure compliance with section 37; and

(b) a new subsection be added, as follows:

"The Review Committee's determination in this regard shall be conclusive".

COMITÉ DE SURVEILLANCE DES ACTIVITÉS
DE RENSEIGNEMENT DE SÉCURITÉ

Modifications à la Loi sur le SCRS

Propositions au Comité spécial de la Chambre des communes 1989

Canada

COMITÉ DE SURVEILLANCE DES ACTIVITÉS
DE RENSEIGNEMENT DE SÉCURITÉ

Modifications à la Loi sur le SCRS

Propositions au Comité spécial de la Chambre des communes 1989

Comité de surveillance des activités de renseignement de sécurité
365, avenue Laurier ouest
C.P. 2430, succursale D
Ottawa (Ontario)
K1P 5W5

(613) 990-8441: Les appels à frais virés sont acceptés et le standard téléphonique est ouvert de 7h30 à 18h00, heure d'Ottawa.

© Ministre des Approvisionnements et Services Canada 1989
No. de cat. JS 71-1/1-1989
ISBN 0-662-56970-9

PREFACE

Un comité spécial de la Chambre des communes, sous la présidence de Blaine Thacker, M.P., a maintenant été créé pour revoir la *Loi sur le Service canadien du renseignement de sécurité*, et la *Loi sur les infractions en matière de sécurité*.

En tant que membres du Comité de surveillance des activités de renseignement de sécurité, «l'organe de surveillance» du Parlement et du public relativement au Service, nous espérons contribuer aux débats du Parlement en faisant des suggestions appropriées, énoncées dans les pages qui suivent, et lorsque nous serons devant ce comité comme témoins.

Après cinq ans d'expérience, nous estimons que la législation sur le SCRS a bien rempli son rôle. Tel que mentionné dans notre rapport annuel de 1987-88, nous croyons toujours que le modèle convenable pour un service de renseignement de sécurité au Canada devrait être:

> Un organisme dont le mandat est énoncé dans une loi plutôt que dans un décret administratif; et qui est assujetti à un véritable contrôle politique et judiciaire et à un examen indépendant.

Cette définition correspond exactement à l'objectif visé par la *Loi sur le SCRS*. Nos suggestions ne sont formulées que pour améliorer la *Loi* et non pour la transformer.

Ronald G. Atkey, c.p., c.r.
Président

Jean Jacques Blais, c.p., c.r.

Frank McGee, c.p.

Saul M. Cherniack, c.p., c.r.

Paule Gauthier, c.p., c.r.

TABLE DES MATIÈRES

Le mandat du SCRS : «s'occuper des menaces envers la sécurité du Canada» 1
Alinéa 2(d) (subversion interne) 1
Alinéa 2(b) (activités influencées par l'étranger) 2
Mettre fin à l'isolement 5
Procédures applicables aux griefs 5
Mandats judiciaires 6
L'avocat du diable 7
Décisions du Cabinet 8
Contrôle des finances 9
Dénonciateurs 9
Audiences à la suite du dépôt d'une plainte 10
Habilitations de sécurité 11
Effets des recommandations du Comité relativement aux plaintes dont il est saisi 13
Accès à l'information et protection de la vie privée 13
La Loi sur la preuve au Canada—I 14
La Loi sur la preuve au Canada—II 14
La question de la responsabilité 16
La collecte de renseignements : établir l'équilibre entre l'offre et la demande 17
Bureau du Renseignement extérieur 20
Divulgation de l'information 21
Ressources humaines 21
Rapports et résumés du Comité 22

MODIFICATIONS À LA LOI DU SCRS

Le mandat du SCRS : s'occuper des «menaces envers la sécurité du Canada»

Tout dans la *Loi sur le SCRS* repose sur la définition de l'expression «menaces envers la sécurité du Canada» figurant à l'article 2. Durant le cours de nos travaux, nous en sommes venus à nous interroger sur la portée et la formulation de cette disposition en particulier.

Menaces envers la sécurité du Canada : alinéa 2 d) (subversion interne)

Témoignant le 17 décembre 1987 en notre nom devant le Comité permanent de la justice et du solliciteur général, le président du CSARS, Ronald G. Atkey précisa que le soi-disant mandat d'antisubversion prévu à l'alinéa 2 *d*) de la *Loi sur le SCRS* s'appliquait «indépendamment de l'improbabilité (que les activités en question) aboutissent à une révolution violente». Il ajouta que «la plupart des enquêtes effectuées par la Direction de l'antisubversion (d'alors) ont été autorisées soit parce qu'on soupçonnait la participation de services du renseignement d'une puissance étrangère hostile, soit parce qu'on craignait une flambée de violence pour des motifs politiques». En insistant pour que la Direction de l'antisubversion soit dissoute, M. Atkey précisa bien que le problème était une question de proportionnalité.

La Direction en question étant maintenant disparue et le solliciteur général exigeant d'autoriser personnellement toute enquête active dans le domaine de l'antisubversion, nous estimons que le temps est maintenant venu de réévaluer cet aspect du mandat du SCRS. En effet, à la lumière de l'expérience acquise avec l'alinéa 2 *d*) de la *Loi*, nous en sommes venus à la conclusion que cette disposition devrait maintenant être abolie. Évidemment, il faudrait, pour la corrélation, abolir en même temps l'alinéa 21(5) *a*) de la *Loi*, lequel traite des mandats en vertu de l'alinéa 2 *d*). Nous nous rendons bien compte que, dans n'importe quelle démocratie, des sources internes peuvent effectivement menacer la sécurité de la nation, mais nous estimons que d'autres dispositions relatives au mandat du SCRS protègent suffisamment la sécurité du Canada.

De plus :

a) L'actuelle *Loi sur le SCRS* fait déjà la distinction entre l'alinéa 2 *d*) et d'autres aspects du mandat en établissant un délai maximum de 60 jours pour l'obtention d'un mandat judiciaire en vertu de cette disposition (paragraphe 21(5) *a*)). Par conséquent, la *Loi* reconnaît déjà que des restrictions particulières sont nécessaires pour les activités menées en vertu de l'alinéa 2 *d*).

b) Dans notre rapport annuel de 1986-1987 (page 40), nous avions déjà dit que dans le domaine de l'antisubversion, une influence étrangère indue et la possibilité de violence pour des motifs politiques sont les critères les plus souvent invoqués. Cependant, d'autres alinéas de l'article 2 sont conçus pour répondre à ces inquiétudes.

c) En 1987, le solliciteur général a annoncé que la Direction de l'antisubversion serait dissoute et que les dossiers qu'on déciderait de conserver seraient tranférés aux directions opérationnelles du Service qui s'occupaient des préoccupations exprimées à l'alinéa 2 *b*).

d) Nous faisons remarquer que, l'an dernier, aucun groupe n'a fait l'objet d'une enquête seulement en vertu de l'alinéa 2 *d*) de la *Loi* (rapport annuel 1987-1988, page 16).

e) La disposition sur l'antisubversion contenue dans la *Loi sur le SCRS* a probablement été critiquée plus que n'importe quelle autre.

1. *Nous recommandons*, par conséquent, d'abroger les alinéas 2 *d*) et 21(5) *a*).

Menaces envers la sécurité du Canada : alinéa 2 b) (Activités influencées par l'étranger)

L'alinéa 2 *b*) de la *Loi sur le SCRS* se lit comme suit :

> les activités influencées par l'étranger qui touchent le Canada ou s'y déroulent et sont préjudiciables à ses intérêts, et qui sont d'une nature clandestine ou trompeuse ou comportent des menaces envers quiconque.

Pour que des activités répondent à cette définition, il faut d'abord qu'elles répondent à des critères essentiels, dont quatre dans le groupe A et le groupe B. Elles doivent :

Groupe A

- être influencées par l'étranger;
- toucher le Canada ou s'y dérouler;
- être clandestines *ou* trompeuses, et
- être préjudiciables aux intérêts du Canada; ou

Groupe B

- être influencées par l'étranger
- toucher le Canada ou s'y dérouler;
- être préjudiciables aux intérêts du Canada et
- comporter des menaces envers quiconque.

Ces critères sont cumulatifs : tous les critères du groupe A ou du groupe B doivent être présents pour que le Service puisse agir. Bien qu'il soit exprimé de façon négative, il existe également un dernier critère. Tout comme pour les alinéas 2 *a*), *c*) et *d*), le Service peut s'impliquer dans les «activités influencées par l'étranger» comprenant des «activités licites de défense d'une cause, de protestation ou de manifestation d'un désaccord» seulement si elles ont un lien avec les activités mentionnées aux alinéas *a*) à *d*). Les critères essentiels énumérés plus haut pour définir le mandat du Service sont des plus ambigus. Ils ne figurent pas dans d'autres lois canadiennes et leur présence dans l'*ASIO Act* de l'Australie a également donné lieu à une controverse considérable. La grande expérience que nous avons de l'application de l'alinéa 2 *b*) nous a amenés à la conclusion que cette disposition devrait être révisée. Nous allons passer en revue, dans l'ordre, les critères essentiels énoncés plus haut.

Activités influencées par l'étranger. La phrase «influencées par l'étranger» pourrait venir de groupements d'intérêts étrangers, d'organisations politiques, de particuliers, d'associations et de sociétés étrangères : en effet, on pourrait à bon droit dire que tous sont «étrangers» du simple fait qu'ils ne soient pas canadiens. On a utilisé ici le verbe «influencer» plutôt que le verbe «diriger», de portée plus étroite, employé dans les directives du Cabinet définissant le mandat du Service de sécurité de la GRC.

Activités qui touchent le Canada ou s'y déroulent. Actuellement, que ces activités se déroulent au Canada, soient dirigées à partir du Canada ou encore qu'elles se déroulent ou soient dirigées à l'extérieur du Canada, il suffit simplement, pour le Service, qu'elles «touchent» le Canada pour répondre au second critère énoncé à l'alinéa 2 *b*). La *Loi* ne dit pas dans quelle mesure une activité en particulier doit «toucher» le Canada pour pouvoir relever de la compétence du Service. Du moment qu'il est possible d'établir «un lien raisonnable» entre l'activité en question et le Canada ou ses intérêts, il ne devient que trop facile de satisfaire à cette condition.

Activités clandestines ou trompeuses. Fondamentalement, il est question ici de secret, de cachette ou de menace. La signification du terme «clandestin» n'est pas très précise : il peut y avoir ici un élément de dissimulation ou de «*male fides*» (mauvaise foi), mais d'après certains dictionnaires, il suffit qu'une activité soit «secrète» pour être «clandestine». Pour éviter toute incertitude, nous proposons d'éliminer «clandestin» et de le remplacer par un mot comme «subreptice», qui transmet plus clairement la notion de dissimulation. La signification de «trompeur» est claire : le terme semble sous-entendre la malhonnêteté en ce sens que la personne qui se livre à des activités trompeuses sait que ce qu'elle dit ou fait est faux et qu'elle cherche délibérément à tromper par ce moyen. Si une puissance étrangère devait s'ingérer «subrepticement» ou «trompeusement» dans les affaires intérieures du Canada, cette ingérence pourrait bien équivaloir à de l'espionnage. Le Service doit alors disposer de tous les moyens nécessaires pour contrer ce genre d'ingérence dans nos affaires intérieures.

Activités préjudiciables aux intérêts du Canada. Le passage le plus discutable de l'alinéa 2 *b*) est l'expression «préjudiciables à ses intérêts» qui ne se retrouve dans une aucune autre mesure législative du Canada. Le critère ici est presque tout à fait subjectif car la *Loi* ne dit pas comment établir ce qui est «préjudiciable». Bien qu'on trouve souvent dans les lois canadiennes des expressions comme «l'intérêt national» ou encore «l'intérêt public», c'est à dessein que le Parlement se sert de ces formules lorsqu'il souhaite donner la plus grande latitude possible à un décideur. En l'occurrence, le Parlement n'a certainement pas voulu donner une telle latitude à un service de sécurité tenu d'assurer un «juste équilibre» entre la nécessité de recueillir des renseignements et le droit de chacun à sa vie privée. Les récentes discussions qui ont eu lieu d'un bout à l'autre du pays sur le bien-fondé de l'Accord de libre-échange montrent bien que même des citoyens bien intentionnés et patriotes peuvent avoir de grandes divergences de vue sur ce qui est «dans l'intérêt du Canada». Nous proposons donc de définir, dans la *Loi*, la signification de l'expression «préjudiciables à ses intérêts».

Activités comportant des menaces envers quiconque. Il y a moins de difficultés avec cette phrase, signifiant comme elle le fait une peur véritable ou la crainte d'une violence physique ou psychologique. Par conséquent, nous suggérons que le mot «menaces» seulement soit qualifié par l'adjectif «graves» (activités graves). Le Parlement a pris cette mesure en

réponse à des inquiétudes semblables en égard du mandat prévu à l'alinéa 2 *c*) relativement à la violence ayant des motifs politiques.

2. *Nous recommandons* de supprimer l'alinéa 2 *b*) de la *Loi sur le SCRS* et le remplacer par le suivant :

«les activités dirigées par l'étranger qui touchent directement le Canada ou s'y déroulent, sont subreptices ou trompeuses et sont préjudiciables à ses intérêts ou comportent de graves menaces envers quiconque.»

Bien que cette formulation de l'alinéa 2 *b*) soit plus étroite, nous estimons qu'elle assurera un mandat suffisant au Service. Elle ne limite pas le Service aux ingérences par des «nations hostiles», ni n'exige que l'ingérence en question se produise au Canada de telle sorte que, par exemple, les activités se déroulant dans nos ambassades à l'étranger seraient couvertes dans la mesure où elles touchent «directement» le Canada. La formulation proposée reconnaît implicitement que des Etats étrangers peuvent agir par l'entremise d'organisations commerciales ostensiblement légitimes et, par conséquent, le Service ne se trouverait pas limité aux seules actions menées par des gouvernements étrangers.

Les agents «involontaires» d'influence, s'ils existent vraiment, ne pourraient plus être ciblés par le Service selon cet alinéa. Toutefois, les étrangers qui essaieraient de «diriger» une ingérence dans les affaires de notre pays feraient de toute évidence l'objet d'un examen par le Service. L'ajout de l'adjectif «graves» devant le mot menaces limiterait la portée de la définition tout en laissant au Service la latitude nécessaire pour s'occuper des menaces qui pourraient se produire soit au Canada, soit à l'étranger (par exemple une menace envers un proche demeuré dans la mère-patrie).

Nous insistons catégoriquement qu'il faut conserver le passage «activités licites de défense d'une cause, de protestation ou de manifestation d'un désaccord» pour limiter cet aspect du mandat du Service de même que la définition en général de ce que sont les «menaces envers la sécurité du Canada».

3. *Nous recommandons également* de définir aussi précisément que possible, dans la *Loi sur le SCRS* modifiée, l'expression «préjudiciables à ses intérêts».

Rédiger des définitions juridiques est compliqué, aussi n'essaierons-nous pas de suggérer une définition précise de l'expression «préjudiciables à ses intérêts». Nous nous contenterons simplement de suggérer des formules qui pourront servir de base aux personnes représentant tous les points de vue lors des prochaines audiences parlementaires.

«préjudiciables à ses intérêts» s'applique aux activités dirigées par l'étranger et/ou sont subreptices ou trompeuses, visant à:

a) porter atteinte à la souveraineté ou l'intégrité territoriale du Canada,

b) affaiblir les défenses militaires du Canada,

c) nuire aux relations internationales du Canada avec un pays ou une organisation,

d) risquer sérieusement la vie, santé ou sécurité des canadiens,

e) obtenir, illégalement ou sans l'autorisation voulue, des renseignements ou des choses classifiées par le gouvernement du Canada dans l'intérêt national, et

f) suborner, contraindre ou corrompre des Canadiens relativement à des activités visées aux alinéas *a*), *b*), *c*), *d*) ou *e*).

Mettre fin à l'isolement

Nous avons noté que le Groupe consultatif indépendant (Comité Osbaldeston) qui a enquêté sur le Service en 1987 a recommandé que «le plan de carrière du personnel du SCRS permette d'évoluer tant à l'intérieur de l'ensemble de l'organisation du renseignement de sécurité que dans la fonction publique en général» (page 20).

Nous estimons que la Direction de l'analyse et de la production du Service, en particulier, aurait grand avantage à ce que des fonctionnaires venus d'autres secteurs de la fonction publique, des universitaires ou encore d'autres personnes ayant des compétences particulières puissent venir y travailler. De leur côté, les analystes et évaluateurs du SCRS ont avantage à pouvoir travailler dans des agences gouvernementales connexes ou encore dans des universités.

Nous nous rendons bien compte qu'il en coûterait quelque chose pour assurer le grand nombre d'habilitations de sécurité nécessaires à toutes les personnes qui passeraient dans le Service, mais nous estimons que les avantages l'emporteraient de loin sur les coûts. Le SCRS croit avoir déjà les moyens d'établir des échanges de personnel avec la Fonction publique.

4. Pour plus de certitude, *nous recommandons* que la *Loi sur le SCRS* soit modifiée expressément pour permettre la rotation, dans le SCRS, de fonctionnaires et d'autres personnes ayant des compétences particulières, sous réserve des dispositions tendant à sauvegarder l'identité des personnes qui s'occupent des activités secrètes du Service.

Procédures applicables aux griefs

Aux termes de la *Loi sur le SCRS*, le CSARS ne peut pas s'occuper des plaintes visées par la procédure de grief énoncée dans la *Loi* ou encore dans la *Loi sur les relations de travail dans la Fonction publique*. La *Loi sur le SCRS* prévoit que certaines plaintes peuvent être entendues par la Commission des relations de travail de la Fonction publique lorsque, par exemple, il s'agit de questions salariales et autres questions du genre qui ne présentent pas grand intérêt pour le CSARS ou à l'égard desquelles il n'a pas de compétence particulière. Toutefois, dans bien d'autres cas, le CSARS pourrait avoir un intérêt vital à la chose, par exemple, si un membre du Service faisait un grief après avoir été accusé d'insubordination pour avoir manifesté fortement sa désapprobation de la façon dont le Service mettait en oeuvre une directive ministérielle touchant un secteur délicat.

5. Par conséquent, *nous recommandons* que le SCRS soit obligé d'informer suffisamment à l'avance le CSARS de toute audience portant sur un grief et tenue conformément au paragraphe 8 (3) de la *Loi sur le SCRS*.

Le CSARS devrait avoir droit à une séance préalable d'information donnée par le SCRS et il devrait avoir le droit aussi d'assister aux audiences sur le grief. De cette façon, le CSARS serait plus en mesure de déterminer si le problème de relations de travail qui fait

l'objet du grief justifie une enquête indépendante dans le cadre des responsabilités propres au CSARS.

Mandats judiciaires

La *Loi sur le SCRS* n'accorde aucune responsabilité précise au CSARS en ce qui a trait aux mandats. Cependant, nous avons signalé des mandats conformément à la fonction générale que nous avons qui consiste à dénoncer tout «usage déraisonnable ou inutile que le Service ferait de ses pouvoirs» (article 40) et à notre responsabilité de «réunir et analyser des statistiques sur les activités opérationnelles du Service» (sous-alinéa 38 *a*) (vii)).

Dans son témoignage devant le Comité permanent de la justice et du solliciteur général, le 20 novembre 1986, M. Atkey fit remarquer que, depuis l'adoption de la *Loi sur le SCRS*, on avait moins de statistiques concernant les mandats que du temps de la *Loi sur les secrets officiels*. Il exprima l'avis que les parlementaires avaient le droit d'être mieux renseignés sur cet aspect. Un autre membre du comité, Jean Jacques Blais, fit remarquer que, puisque c'était le rôle du comité d'examiner les affidavits à l'appui d'un mandat et de vérifier leur justification, le CSARS serait en mesure, finalement, de donner aux Canadiens l'assurance générale que la *Loi* est bel et bien respectée. Nous avons, dans nos trois rapports annuels les plus récents (1985-1986, pages 22-23; 1986-1987, page 13 et 1987-1988, pages 22 et 64), exprimé nos préoccupations à cet égard.

Aux termes de la *Loi sur les secrets officiels*, chaque mandat n'autorisait l'emploi que d'une seule technique secrète contre une seule cible, tandis qu'aux termes de la *Loi sur le SCRS*, un mandat peut autoriser l'utilisation de nombreuses techniques contre de nombreuses cibles. Nous ne pensons pas qu'il soit bien utile d'avoir des statistiques générales sur le nombre de mandats décernés en vertu de la présente Loi. Les graves préoccupations que nous inspire la protection du droit à la vie privée garantie par la *Charte canadienne des droits et libertés* nous portent à formuler la recommandation qui suit.

> 6. *Nous recommandons* que la *Loi* soit modifiée de façon à préciser clairement que le CSARS a la responsabilité de réunir et d'analyser les statistiques concernant les mandats et que le CSARS est tenu de publier chaque année des statistiques concernant le nombre de citoyens canadiens ou d'immigrants reçus qui ont fait l'objet, de la part du Service, d'une surveillance autorisée par mandats judiciaires.

A plusieurs reprises déjà, nous avons parlé du problème des mandats d'urgence (rapport annuel de 1985-1986, page 54; rapport annuel de 1986-1987, page 14; rapport annuel de 1987-1988, page 61). La procédure complexe actuellement en vigueur est une sauvegarde importante, mais nous pensons que, dans certains cas d'urgence, suivre la procédure habituelle pourrait être trop long. Du temps de la *Loi sur les secrets officiels*, on pouvait obtenir un mandat en trois heures environ.

> 7. *Nous recommandons* que l'article 21 de la *Loi sur le SCRS* soit modifié de façon à permettre au directeur du Service d'émettre, avec l'accord du solliciteur général dans chaque cas, un mandat à court terme, non renouvelable, qui devrait être appuyé, dans les 96 heures, d'une demande à la Cour fédérale. Il devrait également être précisé que le CSARS doit être avisé, dans la semaine qui suit, du dépôt d'une demande.

Relativement aux mandats toujours, nous avons également soulevé la question des communications entre un avocat et son client (rapport annuel de 1986-1987, pages 22-23; rapport annuel de 1987-1988, page 62). Ces communications sont protégées par les conditions des mandats en interdisant l'interception de ces communications à l'étude ou à la résidence de l'avocat ou à tout autre endroit où un avocat rencontre habituellement ses clients. De plus, l'interception des appels entre une cible et son avocat est restreinte aux seuls appels dont le directeur du Service ou un directeur général régional ont déterminé qu'ils avaient rapport à la menace énoncée dans le mandat.

Nous sommes heureux que de telles conditions soient habituellement comprises dans les mandats, mais nous préférerions que ces sauvegardes figurent dans la loi même. Le *Code criminel* protège explicitement, par exemple, les communications entre un avocat et son client. Évidemment, nous nous rendons compte qu'il peut y avoir des avocats parmi les terroristes ou les groupes dont les activités menacent la sécurité du Canada. Ce qui nous intéresse, c'est de protéger le genre de communications qui sont effectivement des communications entre avocats et clients. Notre proposition ne concerne que les communications avec des avocats qui agissent comme conseillers juridiques légitimes.

8. *Nous recommandons* d'ajouter un article à la Partie II de la *Loi sur le SCRS* afin de protéger les communications entre un avocat et son client.

9. De plus, *nous recommandons* d'ajouter un autre article à la Partie II de la *Loi sur le SCRS* où seraient énumérées les limites aux mandats dont les juges de la Cour fédérale tiendront compte.

L'avocat du diable (Amicus Curiae)

Depuis 1987, un avocat du ministère de la Justice relevant du sous-solliciteur général du Canada est chargé de contester, devant le Comité d'examen des demandes de mandat, en tant qu'«avocat du diable».* Mais cette personne a un mandat plus restreint que nous avions prévu lorsque nous avons recommandé la nomination d'un avocat du diable dans notre rapport de 1986-87 (page 11).

Présentement, l'avocat du diable ne fait que s'assurer que les renseignements dont le SCRS a l'intention d'utiliser pour la demande de mandat soient exacts. Nous nous attendions à quelqu'un qui contesterait le besoin d'obtenir un mandat—quelqu'un qui présenterait le cas de la même façon que la cible visée le ferait. (La cible, bien entendu, ne sait pas qu'un mandat est demandé contre elle.)

Nous avons des inquiétudes en ce qui concerne le moment de participation de l'avocat du diable au processus. Comme il fait partie du Comité d'examen des mandats judiciaires, l'avocat du diable peut facilement passer pour un pion et au pire, pour un(e) «vendu(e)». Nous croyons que l'avocat du diable devrait intervenir devant la Cour fédérale elle-même.

* L'«avocat du diable» est un avocat chargé de contester un point de vue, avec lequel il ou elle est ou n'est peut-être pas d'accord personnellement, afin que tous les aspects de la question soient considérés.

Malgré que nous sachions que le système paraît fonctionner bien mieux qu'avant, nous estimons qu'une réforme s'impose pour mieux servir la justice naturelle, tant en apparence qu'en substance.

10. *Nous recommandons* que la Partie II de la *Loi sur le SCRS* soit modifiée par l'ajout d'un article stipulant qu'un «avocat du diable» nommé par la Cour soit présent chaque fois que la Cour fédérale est saisie d'une demande de mandat judiciaire.

11. *De plus, nous recommandons* que, lorsque c'est possible, cet avocat ne soit pas un fonctionnaire mais soit choisi parmi une liste d'avocats de l'extérieur qui ont l'habilitation de sécurité nécessaire.

Le CSARS a lui-même une liste d'avocats remplissant les conditions nécessaires. Pour éviter tout conflit d'intérêts, ces avocats seraient nommés par ordre alphabétique ou par un quelconque autre procédé faisant appel au hasard. Le nombre total de nouveaux mandats ou de mandats renouvelés chaque année a diminué de façon importante, aussi la méthode que nous proposons ne devrait pas surcharger les ressources.

Décisions du Cabinet

L'impossibilité dans laquelle nous sommes d'examiner les décisions du Cabinet qui touchent au SCRS s'est avérée un problème dans un cas — dont nous sommes au courant. Durant la période 1988-89, on nous a refusé l'accès au Plan opérationnel pluriannuel, (POP) du SCRS parce que ce document est préparé pour le Conseil du Trésor, un comité du Cabinet. Dans ce cas nous avons fait un compromis : bien que nous n'ayons pas vu le document lui-même, nous avons eu les renseignements qu'il contenait.

Nous avons reçu, du ministère du solliciteur général, l'assurance que les décisions du Cabinet seront reformulées et transmises au CSARS et que nous les recevrons sous forme de directives ministérielles, instruments qui nous sont automatiquement transmis aux termes du paragraphe 6 (2) de la *Loi sur le SCRS*. Toutefois, nous n'avons aucun moyen de savoir si toutes les décisions seront bel et bien transmises, ni si les solliciteurs généraux à venir consentiront au maintien de cette pratique.

Comme nous l'avons dit dans notre rapport annuel de 1987-1988, ceux d'entre nous qui ont déjà fait partie d'un cabinet ne peuvent comprendre pourquoi la Loi empêche le Comité de voir les décisions du Cabinet qui touchent aux opérations du SCRS. A notre avis, les dispositions actuelles créent une suspicion publique inutile.

Nous sommes bien conscients que nous ne devrions pas avoir accès aux dossiers qui révèlent la façon dont le Cabinet a pris ses décisions. Toutefois, les décisions du Cabinet elles-mêmes sont les instruments par lesquels tous les ministères et organismes justifient leurs activités. Il est donc essentiel que le CSARS ait accès aux documents du Cabinet qui concernent le SCRS pour pouvoir véritablement évaluer la mesure dans laquelle celui-ci s'acquitte de ses responsabilités et fonctions. Nous estimons par conséquent que toutes les décisions du Cabinet actuellement en la possession du SCRS et qui ont trait aux responsabilités, fonctions ou ressources du Service devraient nous être accessibles. De même, nous devrions avoir accès à tous les memoranda au Cabinet préparés par le Service ou qui le concernent. De toute évidence, il serait interdit aux membres du Comité de surveillance de

révéler à des tierces parties le contenu des documents confidentiels du Cabinet. Les membres du Comité sont des conseillers privés et ont prêté le même serment que les membres présents et passés du Cabinet.

12. *Nous recommandons* d'abroger le paragraphe 39(3) de la *Loi sur le SCRS* afin de permettre au Comité de surveillance des activités de renseignement de sécurité d'avoir accès à tous les renseignements en la possession du Service, indépendamment de leur provenance.

Le Parlement pourrait aussi modifier le paragraphe 31(2) afin de permettre à l'Inspecteur général d'avoir accès à tous les renseignements en la possession du Service, y compris les documents confidentiels du Cabinet.

Contrôle des finances

Au Canada, le vérificateur général a, par le passé, vérifié les comptes du Service de sécurité de la GRC et, puisqu'il lui incombe de vérifier l'utilisation de toutes les sommes provenant du Trésor (Fonds du revenu consolidé), il est tenu de vérifier en même temps les comptes du SCRS. Ses vérificateurs ont tous l'habilitation de sécurité nécessaire pour faire le travail. Maintenant que les recommandations du Comité Osbaldeston ont été mises en oeuvre, nous pensons que le temps est venu de vérifier les comptes du Service. En effet, nous estimons hautement désirable que le Comité joue un certain rôle dans cette vérification, étant donné la compréhension qu'il a des aspects pratiques du mandat du Service.

Aux termes de l'article 38 de la *Loi sur le SCRS*, le Comité de surveillance n'est pas spécifiquement habilité à évaluer l'administration financière du Service, mais seulement à «surveiller la façon dont le Service exerce ses fonctions». Le Comité estime que ce pouvoir est techniquement suffisant pour lui permettre d'évaluer la gestion financière du Service.

13. Néanmoins, et pour plus de sûreté, *nous recommandons* d'ajouter à l'article 38 de la *Loi* un sous-alinéa précisant que le Comité de surveillance des activités de renseignement de sécurité est habilité à effectuer, en coopération avec le vérificateur général, une vérification financière du Service.

Dénonciateurs

Récemment, nombre de gouvernements ont essayé de supprimer les éventuels obstacles que pourraient rencontrer les fonctionnaires désireux de dénoncer les activités qu'ils estiment être menées à mauvais escient. Les États-Unis ont une loi dite «*Whistleblowers' Protection Act*» (*Civil Service Reform Act*, 1978, 5 U.S.C. s. 7701 *et seq.*) Une mesure semblable est proposée en Ontario et, au palier fédéral, une mesure de protection du genre a été prévue dans la récente *Loi canadienne sur la protection de l'environnement (LCPE)* (Art. 58(4) de cette *Loi* est le S.C. 1988, c.22). Comme nous l'avons dit dans notre rapport annuel de 1987-1988 (page 63) il y a, au Royaume-Uni, un fonctionnaire spécialement chargé de recevoir les «fuites» provenant de membres du MI-5 qui ne sont pas tenus de s'identifier.

La *Loi sur le SCRS* ne protège pas contre les mesures disciplinaires, les employés du Service qui dénonceraient au Comité de surveillance des infractions à la loi. En effet, ces personnes doivent d'abord parler au directeur du Service, qui est, peut-être, précisément la personne à éviter.

> 14. Par conséquent, *nous recommandons* que la *Loi sur le SCRS* soit modifiée par l'ajout d'un paragraphe (3) à l'article 41 afin de garantir l'anonymat aux employés du SCRS qui portent plainte auprès du CSARS et afin aussi de garantir que, si ces personnes étaient finalement identifiées, elles ne feraient l'objet d'aucune mesure disciplinaire uniquement pour avoir porté plainte.

Audiences à la suite du dépôt d'une plainte

La *Loi sur le SCRS* prévoit que le CSARS doit tenir ses audiences en privé. Le paragraphe 48(2) de la Loi ne reconnaît à personne le droit d'être présent lorsque quelqu'un fait des observations au Comité. En 1985, le Comité a adopté une procédure tout à fait détaillée pour les enquêtes relativement aux plaintes dont il est saisi. Une procédure distincte a été établie pour les plaintes relativement au refus d'une habilitation de sécurité pour fin d'emploi de même que pour les affaires d'immigration et de citoyenneté. Le Comité est habilité à établir ces procédures en vertu du paragraphe 39(1) de la *Loi*. Les mesures de sauvegarde détaillées que le Comité a établies et diffusées dans le public sont en contraste frappant avec la procédure souvent abrégée qu'utilise, par exemple, un administrateur général ou une institution gouvernementale avant d'en venir à la décision de refuser une habilitation de sécurité. Habituellement, le CSARS fait une vaste enquête et l'audience qui en résulte souvent ressemble habituellement à la séance d'un tribunal administratif exerçant des pouvoirs quasi-judiciaires.

Lorsque rendre publics les éléments de preuve sur le point d'être produits pourrait porter atteinte à la sécurité nationale, en révélant peut-être des sources de renseignements qui constitueraient «une menace envers la sécurité du Canada», le plaignant et son avocat sont priés de sortir de la salle d'audience pendant que le Comité entend la preuve. La façon de procéder du Comité a fait l'objet de plusieurs contestations devant la Cour fédérale mais, jusqu'ici, aucune n'a eu de succès et les règles de procédure du Comité ainsi que les pratiques qui en découlent ont passé le test lorsque comparés à la *Charte des droits et libertés* ainsi qu'aux exigences d'une procédure équitable. De toute évidence, le Comité serait tenu de se plier au jugement que la Cour pourrait éventuellement rendre.

En cours d'audience, le membre du Comité qui entend le cas peut, à sa discrétion, décider de faire sortir une partie de la salle pendant que l'autre témoigne. Le Comité rappelle alors la partie exclue (habituellement le plaignant) et son avocat et leur expose les grandes lignes de la preuve qui vient d'être présentée, sans rien divulguer de ce qui peut avoir trait à l'intérêt national. Les deux personnes peuvent alors poser des questions et, lorsque c'est possible, contre-interroger le témoin à partir du résumé qui vient de leur être fait.

Nous estimons que la procédure établie par le Comité permet à l'avocat de jouer un rôle passablement équitable et efficace. Pendant que les parties exclues sont en-dehors de la salle d'audience, l'avocat du Comité, qui a reçu des instructions expressément en ce sens,

pose aux témoins du Service les questions que leur poserait normalement l'avocat du plaignant et les contre-interroge avec un zèle égal. Le résumé qui est ensuite présenté à la partie exclue est habituellement négocié par l'avocat du SCRS et du CSARS, sous la surveillance membre qui préside l'audience. Habituellement, le plaignant et son avocat en apprennent suffisamment pour être renseignés aussi complètement que possible sur les arguments qui peuvent être invoqués contre le plaignant.

Nous n'avons rencontré qu'un seul problème avec la formulation actuelle de la *Loi* en ce qui concerne les enquêtes. Le paragraphe 48(2) dit en effet ce qui suit :

> 48.(2) Au cours d'une enquête relative à une plainte présentée en vertu de la présente partie, le plaignant, le directeur et l'administrateur général concerné doivent avoir la possibilité de présenter des observations et des éléments de preuve au Comité de surveillance ainsi que d'être entendus en personne ou par l'intermédiaire d'un avocat; toutefois nul n'a le droit absolu d'être présent lorsqu'une autre personne présente des observations au Comité, ni d'en recevoir communication ou de faire des commentaires à leur sujet.

On a prétendu que, puisque le paragraphe peut s'interpréter comme ne reconnaissant pas le droit d'être présent lors de la présentation des «observations» seulement, cette limite ne s'appliquait pas à la présentation de la preuve ou aux comparutions en personne. Si les tribunaux accueillaient cette interprétation, il deviendrait pratiquement impossible au Comité de surveillance de faire enquête relativement à des renseignements classifiés touchant la sécurité nationale.

Nous estimons que la prétention n'est pas bien fondée mais qu'il serait quand même utile de reformuler le paragraphe 48(2) afin d'en bien préciser le sens.

> 15. *Nous recommandons*, par conséquent, d'ajouter les mots «preuve alléguée, ou déclarations faites» au paragraphe 48(2), de façon qu'il stipule :
>
> ...toutefois nul n'a le droit absolu d'être présent durant, ni d'en recevoir communication ou de faire des commentaires sur les observations présentées, *preuve alléguée, ou déclarations faites* au comité de surveillance par toute autre personne.

Habilitations de sécurité

Sans habilitation de sécurité, toute personne perd des chances d'emploi tant dans le secteur public que dans le secteur privé. La *Loi sur le SCRS* n'autorise l'intéressé à présenter une plainte au Comité (article 42) que dans certains cas.

Premièrement, il faut que l'intéressé ait fait l'objet d'une décision de renvoi, de rétrogradation, de mutation ou d'opposition à un engagement, avancement ou mutation ou encore à un contrat de fournitures ou de services à l'État du seul fait de n'avoir pas obtenu l'habilitation de sécurité nécessaire. Comme nous le disions dans notre rapport annuel de 1987-1988 (page 60), l'article est actuellement formulé de façon telle que si quelqu'un est écarté d'un emploi ou alors congédié par un entrepreneur fédéral pour supprimer un obstacle à l'obtention d'un marché avec l'État, cette personne n'a pas de véritable recours. En outre,

si l'intéressé n'a pas l'habilitation de sécurité nécessaire pour avoir accès à certaines installations fédérales, par exemple un aéroport, il ne lui est pas possible d'avoir l'emploi désiré et dans ce cas, elle n'a pas non plus de recours auprès du Comité.

Deuxièmement, la décision de refuser une habilitation de sécurité doit venir de «l'administrateur général».

Troisièmement, le droit de porter plainte lui-même repose sur le «refus» de quelque chose. Or, le terme peut s'interpréter d'une façon étroite au point que seul un refus catégorique pourra donner à l'intéressé le droit de porter plainte en vertu de la Loi. Mais, qu'arrive-t-il si les autorités font traîner les choses en longueur sans jamais opposer de refus formel? Actuellement, l'intéressé peut s'adresser au Comité de surveillance en vertu de l'article 41, mais la Loi devrait peut-être prévoir une meilleure protection contre les retards déraisonnables dans la prise d'une décision.

Quatrièmement, la perte d'une occasion d'emploi doit être attribuable, aux termes de la *Loi*, à «la seule raison du refus d'une habilitation de sécurité». Qu'arrive-t-il cependant si l'employeur peut affirmer de bonne foi qu'il y avait d'autres motifs, bien que tout à fait mineurs? L'argument a été présenté dans deux contestations au moins qui ont été faites relativement à la compétence du Comité de faire enquête au sujet d'une plainte.

Nous estimons que toute personne à qui une habilitation de sécurité est refusée devrait avoir le droit de porter plainte auprès du Comité de surveillance. Il ne devrait pas y avoir de catégories de Canadiens ou d'immigrants reçus qui, pour une même raison, ont le droit de porter plainte auprès du Comité tandis que d'autres n'ont pas ce droit. Dans le monde d'aujourd'hui, ne pas avoir son habilitation de sécurité se répercute immédiatement sur l'emploi et, à long terme, affecte les chances d'emploi.

Quoi qu'il en soit, outre les répercussions sérieuses qu'un refus d'habilitation de sécurité a sur les chances d'emploi, la loyauté d'un citoyen canadien ou d'un immigrant reçu ne devrait jamais être remise en cause au point qu'une habilitation de sécurité lui soit refusée sans que l'intéressé n'ait automatiquement le droit d'exiger que le Comité de surveillance fasse enquête sur son cas.

Souvent, l'habilitation de sécurité est totalement refusée, *à quelque niveau que ce soit*, mais dans certains cas, des personnes qui auraient besoin d'une cote TRES SECRET ne reçoivent que la cote SECRET ou CONFIDENTIEL, ce qui a habituellement sur l'emploi de l'intéressé le même effet que le refus catégorique de n'importe quel niveau d'habilitation de sécurité aurait eu.

Les modifications que nous proposons donneraient à tout citoyen canadien ou immigrant reçu le droit d'exiger une enquête du Comité de surveillance au niveau requis.

16. *Nous recommandons* que les paragraphes 42(1) et (2) soient abrogés et remplacés par la disposition suivante :

«42.(1) Lorsqu'une habilitation de sécurité exigée, pour n'importe quel motif, par le gouvernement du Canada est refusée à quelqu'un ou lui est accordée à un niveau inférieur au niveau nécessaire ou qu'elle est ramenée à un niveau inférieur au niveau nécessaire, l'administrateur général ou la personne qui a pris cette décision doit, dans

les dix jours suivant la prise de la décision, envoyer à l'intéressé un avis l'informant qu'une habilitation de sécurité du niveau requis lui a été refusée et qu'il a le droit, en vertu du présent article, d'en appeler de cette décision auprès du Comité de surveillance des activités de renseignement de sécurité.»

Il faudrait apporter quelques modifications corrélatives au reste de l'article 42.

Effet des recommandations du Comité relativement aux plaintes dont il est saisi

Actuellement, la Cour fédérale du Canada est à nouveau saisie de la cause *Thomson*; la cour d'appel et la division de première instance ne s'entendent pas sur la question de savoir si les recommandations du Comité concernant l'habilitation de sécurité sont exécutoires pour l'administrateur général. Indépendamment de la décision que prendra éventuellement le tribunal, le Parlement pourrait vouloir clarifier son intention à l'occasion de l'examen de la *Loi sur le SCRS* après cinq ans d'expérience.

Nous faisons remarquer, en passant, que dans l'*ASIO Act* de l'Australie, les «conclusions» du tribunal d'appel en matière de sécurité ont préséance sur la décision originelle concernant l'habilitation de sécurité (article 61).

Nous estimons que le Parlement n'irait nullement à l'encontre de la responsabilité ministérielle s'il décidait d'habiliter le Comité de surveillance des activités de renseignement de sécurité à trancher les cas où il n'est pas d'accord avec la décision d'un administrateur général de refuser une habilitation de sécurité. Les décisions qui déterminent en fait si l'intéressé pourra travailler dans le domaine qu'il a choisi, ont des répercussions directes sur ses droits. Obtenir gain de cause auprès d'un tribunal neutre comme le CSARS pour apprendre ensuite que son habilitation de sécurité continue à être refusée par un administrateur général qui a toute latitude pour cela, doit être profondément décourangeant.

Finalement, la Politique et procédures de sécurité du gouvernement qui date de juin 1986 précise que tous les fonctionnaires à qui une habilitation de sécurité a été refusée peuvent s'adresser au Comité de surveillance des activités de renseignement de sécurité. Nous en déduisons que, de toute évidence, le Comité est bel et bien habilité à rendre des décisions.

17. Par conséquent, *nous recommandons* que le paragraphe 52(2) de la *Loi* soit modifié de façon que les décisions rendues par le Comité concernant les habilitations de sécurité soient sans appel et exécutoires pour l'administrateur général.

Accès à l'information et protection de la vie privée

Dans le cours normal des choses, les pouvoirs du Comité de surveillance des activités du renseignement de sécurité recouperont presque certainement les pouvoirs détenus par le commissaire à l'information ou par le commissaire à la protection de la vie privée. La chose s'est déjà d'ailleurs produite dans le cas du second.

Il se peut que, faisant enquête au sujet d'une plainte déposée en vertu de la *Loi sur l'accès à l'information* ou encore de la *Loi sur la protection des renseignements personnels*, l'un ou l'autre commissaire entame, avec le Service, des négociations portant peut-être sur les

dossiers mêmes que le Comité souhaite examiner dans l'exécution de ses propres responsabilités. Le Comité estime qu'en pareil cas, il ne faut en rien entraver les travaux de l'un ou l'autre commissaire du seul fait que le CSARS fait enquête, ou vice versa. En effet, chaque organisme a ses propres responsabilités dont il doit s'acquitter. Bien que, à notre avis, l'actuelle formulation de la *Loi* assure largement et en toutes circonstances au CSARS l'accès nécessaire aux dossiers voulus, certaines autorités gouvernementales n'en sont pas tout à fait convaincues.

18. Par conséquent, *nous recommandons* que le Parlement examine s'il serait bon de clarifier la question en ajoutant, au paragraphe 39(2) de la *Loi sur le SCRS*, un alinéa précisant que le Comité est habilité à avoir accès à tous les renseignements en possession du Service, indépendamment de toute enquête entreprise par le commissaire à l'information ou par le commissaire à la protection de la vie privée.

Lois connexes : la Loi sur la preuve au Canada — I

Témoignant le 20 novembre 1986 devant le Comité permanent de la justice et du solliciteur général, le président répondit à une question concernant l'article 37 de la *Loi sur la preuve au Canada*, lequel prévoit que, dans les instances criminelles, un membre du SCRS peut s'opposer à la divulgation de renseignements devant le tribunal. Cette disposition a été très critiquée et M. Atkey a déclaré «qu'à l'intérieur du Service, on n'était pas très à l'aise avec la formulation et l'application de cet article», et que lui-même y voyait un problème (page 2:16). Il a alors émis l'opinion que c'était là un point sur lequel les autorités devraient s'attarder durant l'examen de la *Loi sur le SCRS*. Il a reconnu que c'était «une procédure terriblement incommode ... (et qu'il y avait) risque de préjudice envers l'accusé dans un procès criminel». Cependant, le Comité est bien conscient des raisons pour lesquelles n'importe quel service de sécurité ferait de son mieux pour tenir secrètes ces sources de renseignement et les «secrets du métier». Nous sommes d'accord que les renseignements obtenus du SCRS devraient rarement être utilisés comme éléments de preuve lors d'un procès à la Cour. Toutefois, nous devons reconnaître qu'il y aura des exceptions et des procédures devraient être disponibles afin de protéger l'intérêt national au besoin.

Dans notre rapport annuel de 1986-1987 (page 30), nous faisions remarquer que l'article 486 du *Code criminel* prévoyait que le public peut être exclu de la salle d'audience pour divers motifs, qui sont énoncés.

19. Conséquemment, *nous recommandons* que l'article 486 du *Code criminel*, soit modifié afin

a) d'ajouter la phrase «menaces envers la sécurité du Canada au sens de l'article 2 de la *Loi sur le SCRS*», afin que le juge puisse avoir le pouvoir d'exclure le public de la salle d'audience durant les parties d'un procès qui pourraient vraisemblablement porter sur des question d'intérêt national; et

b) de permettre au juge d'exclure le défendeur et son avocat ainsi que le public de la salle d'audience lorsque des questions d'intérêt national sont soulevées.

La Loi sur la preuve au Canada — II

Jusqu'à ce que la *Loi sur la preuve au Canada* soit modifiée, au début des années 1980, le solliciteur général pouvait signer un certificat attestant que la divulgation de certains renseignements nuirait à la sécurité nationale. L'instrument était sans appel et ne pouvait être contesté devant aucun tribunal.

L'article 38 prévoit maintenant une procédure par laquelle une objection écrite ou verbale à la divulgation de renseignements susceptibles de porter préjudice à la sécurité nationale peut être portée en appel devant le juge en chef de la Cour fédérale ou tout autre juge désigné par lui ou elle. En d'autres termes, l'examen des renseignements en question ne peut être fait que par une personne bien précise ou encore par la personne désignée par celle-ci, et doit s'effectuer à huis clos et dans la région de la capitale nationale.

On a voulu, de la sorte, mieux protéger les droits des personnes participant à une instance criminelle devant les tribunaux. Toutefois, la procédure a causé certains problèmes après la création du Comité de surveillance en juillet 1984.

Il arrive que les recommandations ou les décisions du Comité soient contestées devant la Cour fédérale d'appel en vertu de l'article 28 de la *Loi sur la Cour fédérale*. Lorsque le cas se produit, il faut obtenir de la Cour des directives particulières afin de protéger les documents qui touchent à l'intérêt national et qui seraient normalement rendus publics si la procédure habituelle était suivie. En outre, lorsque le ministère de la Justice s'oppose à ce que des renseignements touchant la sécurité nationale soient divulgués à l'appelant, la Cour doit alors attendre la décision du juge désigné par le juge en chef quant à la validité de l'objection visant la «sécurité nationale». La décision rendue par le juge désigné peut être portée en appel devant la Cour fédérale d'appel et les juges de cette cour peuvent alors examiner les documents en question. Ironiquement, cependant, s'il n'y a pas d'appel, la Cour d'appel ne peut pas examiner les documents.

Ce processus complexe fait partie de la procédure qui a pour but de reviser les recommandations et décisions formulées par le Comité de surveillance après une enquête. Dans le cadre d'une enquête du genre, le Comité de surveillance examine tous les documents, indépendamment de leur cote, et entend les témoignages verbaux, qu'ils concernent ou non la «sécurité nationale». Aucun renseignement classifié n'est transmis au plaignant au cours de l'enquête effectuée par le Comité.

Étant donné que les recommandations ou décisions du Comité sont très souvent fondées, pour la plus grande partie, sur des renseignements qui concernent la «sécurité nationale», le tribunal qui est chargé de reviser les conclusions formulées par le Comité et la procédure qu'il a suivie ne peut le faire véritablement que s'il a aussi accès à tous les renseignements qu'a examinés le Comité de surveillance.

> 20. Par conséquent, *nous recommandons* que la *Loi sur le SCRS* soit modifiée de telle sorte que, en cas d'examen judiciaire, la Cour fédérale d'appel soit la seule à avoir compétence en vertu de l'article 28 de la *Loi sur la Cour fédérale*, et soit habilitée à examiner tous les rapports effectués par le Comité de surveillance en vertu de l'article 42 ou n'importe quel rapport touchant les droits d'une personne effectué en vertu de l'article 41, de même que tous les documents pertinents.

21. *Nous recommandons de plus* qu'une procédure spéciale soit établie, soit par loi ou par règlement, pour permettre la communication à la Cour fédérale d'appel des dossiers et des documents du Comité de surveillance, sans que la nature de ces documents soit rendue publique et, si nécessaire, sans que l'existence ou la non existence de ces dossiers soit reconnue.

L'adoption de ces recommandations aurait l'heureux effet d'éliminer la nécessité, pour quelqu'un, de contester, en vertu de l'article 18 de la *Loi sur la Cour fédérale*, une décision rendue par le Comité de surveillance. La procédure actuelle est injuste en ce que l'intéressé ne sait habituellement pas grand-chose de ce qu'on lui reproche et n'a que très peu de chances d'être capable de prouver le bien-fondé d'un appel. Conséquemment, la plupart des personnes qui portent plainte en vertu de l'article 41 de la *Loi sur le SCRS* ne sont pas en mesure de contester efficacement une décision du Comité de surveillance.

La question de la responsabilité

Après cinq années d'existence, le Comité s'est formé des opinions bien arrêtées quant à l'efficacité et à l'utilité des institutions établies par la *Loi*. Chez nous, cas unique, la responsabilité du Service incombe au solliciteur général, qui rend lui-même compte au Parlement. Mais la *Loi* prévoit également l'existence d'un inspecteur général à plein temps, chargé de contrôler les activités du Service au nom du ministre et l'assiste dans sa responsabilité du SCRS. Le CSARS complète le tableau : il s'agit d'un comité tripartite, composé de membres à temps partiel, sans lien avec l'administration du jour. A notre avis, la composition tripartite du Comité qui est formé de conseillers privés à temps partiel, a bien fonctionné jusqu'ici. Nous avons habituellement réussi à atteindre le consensus et à ramener la «partisanerie» au minimum. Autre avantage : comparativement à d'autres organismes de surveillance de l'étranger, nous n'avons pas eu de problème avec les «fuites».

22. *Nous recommandons* que la *Loi sur le SCRS* conserve le Comité de surveillance des activités de renseignement de sécurité dans ses fonctions actuelles.

L'autre solution serait, évidemment, de créer un comité parlementaire permanent pour surveiller les activités du SCRS. Aux États-Unis, le Congrès a deux comités du genre. En Australie, on a récemment nommé des parlementaires au comité parlementaire mixte chargé de s'occuper de l'organisation australienne du renseignement de sécurité; cependant ce comité est quelque peu limité dans son accès aux documents retenus par l'ASIO. De plus, la Commission McDonald a recommandé la création d'un comité parlementaire mixte de surveillance. Quoi qu'il en soit, nous estimons que la formule du CSARS a eu du succès jusqu'ici et nous proposons que le Comité soit maintenu, dans une *Loi sur le SCRS* renouvelée, dans sa fonction de principal organisme de surveillance. Nous formulons à cet égard la recommandation suivante :

23. *Nous recommandons* d'inclure dans la *Loi sur le SCRS* une disposition obligeant le directeur du Service à offrir de tenir régulièrement des consultations avec les chefs des principaux partis d'opposition représentés au Parlement de façon à les tenir au courant de ce qui concerne la sécurité.

On trouve une disposition du genre dans l'*ASIO Act* (article 21) et, à notre connaissance, la chose marche bien. Ceci renforçerait le rôle du Parlement dans la hiérarchie des responsabilités.

Le CSARS devrait-il être habilité à examiner les activités de tous les autres éléments du réseau canadien de renseignement? Dans l'annexe C de notre rapport annuel de 1987-1988, nous avons donné les principaux éléments de ce réseau. Témoignant le 3 juin 1986 devant le Comité permanent de la justice et du solliciteur général, M. Atkey déclara que «c'était là une question que le Parlement devrait aborder un jour ou l'autre» (page 21:25). M. Atkey n'aborda cependant pas la question de savoir s'il faudrait élargir les fonctions de surveillance du CSARS.

En Australie, il existe un organisme indépendant de surveillance pour tout le réseau australien de renseignement de sécurité. C'est l'office de l'inspecteur général du renseignement et de la sécurité qui est responsable de «la surveillance et de l'examen de la mise en application de la loi par les organismes australiens de renseignement ou de sécurité, ainsi que de la pertinence de leurs activités particulières» (*The Inspector General of Intelligence and Security Act*, 1986, article 4). Cet office assure la surveillance des homologues australiens du SCRS, c'est-à-dire le Communications Security Establishment, l'Office of National Assessments, les différentes directions du renseignement et de la sécurité du ministère de la Défense nationale ainsi que l'ASIS, l'homologue australien de la CIA.

Aux États-Unis, la situation est bien sûr identique à ce qu'on trouve en Australie : tous les organismes de renseignement sont assujettis à la surveillance de comités du Congrès.

La Commission McDonald avait recommandé que l'organisme de surveillance dont elle proposait la création s'occupe de tous les organismes fédéraux chargés de recueillir clandestinement des renseignements, à l'exception de la GRC. (Récemment, la GRC a reconnu la création d'une Section des enquêtes relatives à la sécurité nationale (SERSN). A prime abord, il ne semble pas y avoir de raison pour laquelle cet organisme ne devrait pas être assujetti à la surveillance d'un organisme externe.) Dans son rapport, la Commission laissait entendre que si l'organisme indépendant de révision n'a pas compétence pour le faire, «il sera trop facile pour le gouvernement d'éviter cet examen en transférant effectivement des responsabilités du service de sécurité à quelque autre organisme qui n'y est pas assujetti». (Rapport de la Commission McDonald, volume 2, page 933.)

Nous faisons remarquer qu'il n'existe encore aucun mécanisme de surveillance pour le reste du réseau canadien de renseignement, si l'on excepte le mécanisme de la responsabilité ministérielle. Évidemment, si le Parlement acceptait notre recommandation de créer un organisme d'évaluation du renseignement (voir page 19), tous les organismes canadiens de renseignement feraient alors l'objet d'un meilleur contrôle du fait de l'existence de cet organisme. Pourtant, ce contrôle ne serait pas comparable à un système d'examen. Nous estimons qu'il serait bon que le Canada suive l'exemple australien et l'exemple américain en instituant, comme le recommande la Commission McDonald, un système d'examen pour tous les organismes fédéraux qui s'occupent de recueillir des renseignements.

> 24. *Nous recommandons* que le Parlement songe à adopter une mesure législative prévoyant un contrôle indépendant de tous les autres éléments du réseau canadien de renseignement.

Nous n'avons pas d'opinion arrêtée sur la question de savoir si cette responsabilité pourrait être assumée par un CSARS plus étendu ou par quelque autre organisme indépendant établi à cette fin.

La collecte de renseignements : établir l'équilibre entre l'offre et la demande

Surtout en un temps où la bonne administration financière arrive au premier rang des préoccupations publiques, les parlementaires ne manqueront pas de s'intéresser à la «rentabilité» du Service. En tant qu'organisme de renseignement, le SCRS recueille-t-il et analyse-t-il de façon efficace l'information pour la transformer en «renseignements» utiles? Le CSARS définit d'ailleurs lui-même cette activité comme «la collecte, tant de sources ouvertes que cachées, et l'analyse de l'information afin d'être averti à l'avance des activités qui peuvent constituer une menace envers la sécurité du Canada».

Il y a deux catégories majeures de renseignements : le renseignement de sécurité, qui peut provenir du pays même ou de l'extérieur, mais qui a toujours trait à des menaces envers la sécurité du Canada, et le renseignement extérieur, qui concerne d'autres pays. Le SCRS est la principale «source» concernant la première catégorie de renseignements.

Le Groupe consultatif indépendant constitué en 1987 pour faire enquête sur le Service (Comité Osbaldeston) a fait une autre distinction utile entre les deux catégories de renseignements. Le *renseignement opérationnel* est «lié aux enquêtes sur des activités considérées comme constituant une menace pour la sécurité du Canada». Il est recueilli surtout (mais non exclusivement) à l'aide de techniques d'enquête, sert à court terme et est obtenu pour des clients bien précis ou à une fin particulière«. *Le renseignement stratégique* »est davantage fondé sur la recherche à l'aide d'informations provenant de toutes les sources disponibles, vise une activité à plus long terme et de portée plus globale, et est destiné à un client interministériel ou au gouvernement dans son ensemble«. Il est »évalué à la lumière d'autres intérêts nationaux du Canada«.

Dans notre rapport annuel de 1987-1988, nous résumions les résultats de notre enquête sur la Direction de l'analyse et de la production du Service. Nous avons conclu qu'il y avait eu amélioration importante mais en remarquant l'insuffisance de sources de renseignement multidisciplinnaire nécessaire pour assurer les éléments économiques, politiques et sociaux requis pour avoir des renseignements stragégiques complets. Par exemple, il n'y a eu jusqu'ici qu'une participation très minime de spécialistes venant de l'extérieur du secteur public. A notre avis, la Direction a encore des progrès à faire si le Service doit produire autre chose que des renseignements essentiellement opérationnels.

Nous signalons au passage que le Comité Osbaldeston s'inquiétait également de la façon dont le Service produisait ces renseignements ainsi que «de l'absence de système coordonné de production». De même, en 1987, le Comité spécial du Sénat sur le terrorisme et la sécurité publique (Comité Kelly) recommandait que «le Secrétariat, renseignement et sécurité du Bureau du Conseil Privé soit agrandi et renforcé pour donner un centre spécial pour la collection des renseignements et l'évaluation des ministères et des agences devant être examinés par le Comité consultatif des renseignements (CCR) et pour la dissémination aux ministères et agences pertinents». (page 62)

Le CCR est «ce qui ressemble le plus au Canada à un organisme unique de collecte, d'analyse, de discussion et de diffusion de l'information et du renseignement concernant la défense et la sécurité». Ses membres coopèrent ensemble et coordonnent la production des renseignements à partir de la recherche et de l'analyse effectuées par des organismes fédéraux, notamment le SCRS, le ministère des Affaires extérieures (MDEA), le ministère de

la Défense nationale (MDN) et le Centre de la Sécurité des télécommunications. Actuellement, le CCR dessert tous les ministères et appuie le Comité du Cabinet chargé de la sécurité et du renseignement, organe par lequel le Premier ministre exerce son leadership et établit les priorités pour les organismes de renseignement de sécurité et de renseignement étranger.

La Commission McDonald a également fait valoir la nécessité de centraliser la fonction d'évaluation du renseignement au Canada, et d'établir un organe central pour s'en charger. A cette fin, la Commission recommandait (deuxième rapport, volume 2, pages 900-903) la création au Bureau du Conseil privé, d'un Bureau d'appréciation des renseignements, qui, cependant, ne serait pas chargé de recueillir l'information. La Commission était d'avis que cet organisme devrait être distinct du Secrétariat de la sécurité et des renseignements, avoir son propre groupe d'analystes, en plus des agents détachés par les ministères et organismes gouvernementaux ayant des responsabilités en matière de sécurité et de renseignements. Le directeur général de cet organisme relèverait du Premier ministre par l'entremise du secrétaire du Cabinet et ferait également partie du Comité consultatif du renseignement.

La Commission insistait cependant pour que l'organisme de renseignement de sécurité (actuellement le SCRS) soit doté de grands moyens d'analyse, lui permettant de produire des appréciations des menaces à court terme et à long terme. Ces appréciations seraient utilisées par le «Bureau» proposé, et ses agents du renseignement prendraient fréquemment part aux travaux des groupes constitués par le Bureau pour établir des évaluations et des priorités à long terme.

Nous avons été favorablement impressionnés par l'Office of National Assessments (ONA) de l'Australie. Dans ce pays, il y a une distinction nette entre les «organismes de collecte» et les «organismes d'appréciation». Créé il y a plus de dix ans, l'ONA est chargé de regrouper et d'évaluer l'information recueillie sur de nombreuses questions politiques, économiques et stratégiques. Le directeur général de l'organisme relève du Premier ministre du pays. L'ONA ne recueille pas d'informations, mais évalue simplement les renseignements qui lui sont transmis par les organismes de collecte appartenant au réseau du renseignement de sécurité du pays, et notamment l'Australian Security Intelligence Organization (ASIO). L'ONA produit également des rapports sur des questions précises afin d'aider les ministres à formuler leurs politiques. Il est conçu comme un organisme autonome chargé de dispenser en toute liberté des conseils objectifs. L'ONA aide également le gouvernement à établir ses priorités en matière de renseignement et demande aux organismes pertinents de recueillir les renseignements précis qui lui manquent. L'organisme emploie des analystes venant à la fois du secteur public et du secteur privé, et notamment des universitaires spécialisés dans des domaines précis. Le directeur de l'ONA précédent, M. Michael Cook, a récemment été nommé ambassadeur de l'Australie à Washington. Il a été remplacé dans ses fonctions par l'ambassadeur de l'Australie au Japon.

> 25. *Nous recommandons* que le Parlement examine la faisabilité et le bien-fondé d'établir un organisme similaire à l'Office of National Assessments de l'Australie.

Un tel Bureau d'appréciation des renseignements serait chargé d'évaluer les renseignements recueillis par le SCRS de même que par le Centre de la Sécurité des télécommunications et du Bureau du Renseignement extérieur du ministère des Affaires extérieures. En outre, il aiderait le Comité du Cabinet chargé de la sécurité et du renseignement à établir

les priorités du gouvernement et contrôlerait la qualité des renseignements générés par tous les organismes fédéraux. Il pourrait, tout comme le SCRS, être établi par une loi. Et tout comme l'ONA, il devrait avoir à son service une équipe «multidisciplinaire» de citoyens qualifiés et notamment des spécialistes venant de l'extérieur de l'administration publique. Il relèverait du Comité consultatif du renseignement.

Bureau du Renseignement extérieur

A l'époque moderne, le Canada n'a pas eu de service secret du renseignement extérieur. Devrions-nous avoir un organisme aussi «offensif» que la CIA aux États-Unis, ou l'Intelligence Service en Australie (ASIS)? Comme nous ne disposons pas des moyens nécessaires pour recueillir, par des voies secrètes, des renseignements concernant l'extérieur, nous devons nous fier à d'autres pays pour obtenir certains renseignements, ce qui peut menacer notre autonomie dans certains cas. Dans la mesure où les sources cachées de renseignement sont un avantage pour s'ouvrir l'accès d'un marché, acquérir une technologie et négocier à l'échelle internationale, le Canada se trouvera donc désavantagé par rapport à ses principaux partenaires commerciaux. Cependant, il n'est pas du tout évident que le Canada ait besoin d'un service secret du renseignement extérieur.

Compte tenu de son éloignement et des difficultés qu'elle éprouvait à obtenir de ses alliés les renseignements extérieurs dont elle avait besoin, l'Australie a créé l'ASIS pour s'occuper des domaines qui intéressent particulièrement le pays. L'organisme recueille donc des renseignements politiques et économiques destinés aux décideurs australiens. Le Canada ne semble pas avoir besoin d'un organisme aussi «offensif» de collecte de renseignements extérieurs. Cependant, les choses se présentent peut-être autrement pour le renseignement de sécurité et peut-être aussi le renseignement criminel qui intéresse le Canada et qui est recueilli à l'étranger.

Le Comité est opposé à la création d'un organisme distinct, «offensif» de collecte du renseignement extérieur pour le Canada. Nous pensons tout simplement que la nécessité n'en a pas été prouvée. Cependant, nous pensons aussi que la Loi sur le SCRS pourrait, du moins, prévoir la possibilité que le SCRS recueille, au besoin, des renseignements extérieurs.

> 26. Par conséquent, *nous recommandons* de supprimer les mots «dans les limites du Canada» de l'article 16 de la *Loi*.

De la sorte, le SCRS serait en mesure d'aider le ministre de la Défense nationale ou le Secrétaire d'État aux Affaires extérieures à recueillir, de n'importe quelle source, des renseignements concernant les capacités, les intentions ou les activités de personnes ou d'États étrangers. Aux termes de cet article, le SCRS ne serait habilité à agir en dehors du Canada que sur «demande personnelle écrite» de l'un ou l'autre ministre, et après avoir également obtenu le consentement écrit du solliciteur général. La modification proposée ne devrait pas empêcher le CSARS d'examiner les opérations du Service, que ce soit au pays même ou à l'étranger.

Toutefois, advenant que le Parlement modifie l'article 16 dans le sens proposé et afin d'éliminer tout doute quant à la compétence du CSARS, nous proposons de modifier également l'article 38.

27. *Nous recommandons* que l'article 38 de la Loi soit modifié afin de bien préciser que le Comité a compétence pour contrôler toutes les opérations du SCRS hors du Canada.

L'adoption des recommandations 26 et 27 ne modifierait pas nécessairement les activités du SCRS. Toutefois, en examinant la possibilité d'apporter la modification proposée, le Parlement pourrait délibérer de la possibilité de donner au SCRS les moyens d'agir dans des cas particuliers.

Divulgation de l'information

L'article 19 de la Loi restreint la communication par le SCRS d'informations recueillies par ses vastes moyens. Nous croyons que la Loi restreint aussi la communication de telles informations par le solliciteur général et ses représentants ainsi que le personnel du ministère du solliciteur général; ils ont accès aux renseignements secrets du SCRS, et s'ils divulgaient ces renseignements ce serait se moquer des dispositions de sécurité soigneusement formulées à l'article 19. Toutefois, bien que nous n'ayons pas de raison de croire à des inconvenances, nous avons appris que le solliciteur général, ses représentants et son personnel ne croient pas être liés par cet article.

28. *Nous recommandons* par conséquent, que les limites prescrites à l'article 19 de la *Loi sur le SCRS* s'appliquent également au solliciteur général, à tous ses représentants, ainsi qu'au personnel du ministère du solliciteur général, ayant accès aux renseignements recueillis par le SCRS dans l'exercice de ses responsabilités et fonctions.

A d'autres égards, toutefois, nous croyons que la disposition relativement à la divulgation devrait être plus élaborée. L'article 19 a une disposition en ce qui concerne la communication d'informations, dans certaines circonstances, à une «personne appartenant à la fonction publique du Canada». On pourrait interpréter cette disposition comme s'appliquant seulement aux agents payés employés selon les conditions de la Loi sur l'emploi dans la fonction publique. Nous croyons que cette disposition devrait comprendre les sénateurs et membres de la Chambre des communes.

29. *Nous recommandons* par conséquent, que l'alinéa 19(2) *d*) de la *Loi sur le SCRS* soit modifié afin de permettre que des informations soient communiquées aux sénateurs et aux membres du Parlement selon les principes établis pour les ministres et une «personne appartenant à la fonction publique du Canada».

Ressources humaines

Comme l'a dit la Commission Mcdonald et comme nous l'avons déjà dit nous-mêmes, la technique d'enquête la plus «importune» est la «source humaine», c'est-à-dire une personne qui informe le Service des activités d'une cible retenue par lui. La «source humaine» peut avoir été recrutée lorsqu'elle se trouvait déjà proche de la cible ou peut avoir été priée de s'en rapprocher en s'infiltrant dans l'organisation de la cible visée ou dans son cercle d'amis. Les sources humaines sont généralement payées selon la valeur des renseignements qu'elles fournissent. Certains ont suggéré que le recours aux sources humaines ne devrait être autorisé que par mandat judiciaire, comme cela se fait pour les autres techniques d'intrusion du genre. Nous estimons, quant à nous, que ce serait là imposer un fardeau

vraiment trop lourd au Service et que, dans bien des cas, le procédé serait difficile à appliquer en pratique.

Il serait difficile par exemple, d'introduire dans un tel processus une source occasionnelle, «itinérante», en voie de formation, et plusieurs sources non rémunérées.

Cependant, nous estimons que le Service devrait être tenu d'observer des lignes directrices ministérielles sévères pour ce qui est du recours à des sources humaines.

30. *Nous recommandons*, par conséquent, que la *Loi sur le SCRS* soit modifiée de façon à stipuler que le solliciteur général peut donner au Service des lignes directrices précises concernant le recours à des sources humaines. Ces lignes directrices seraient automatiquement transmises au Comité de surveillance en vertu du paragraphe 6(2) de la *Loi*.

Rapports et résumés du Comité

L'article 55 de la *Loi sur le SCRS* prévoit qu'il doit y avoir consultation entre le Comité de surveillance et le directeur du Service lorsque le Comité de surveillance est en train de préparer certains rapports de sorte qu'ils soient conformes aux exigences de l'article 37 de la Loi. Bien que l'intention de l'article soit clair pour nous, il n'y est cependant pas précisé que, en cas de désaccord, la décision finale quant au contenu du rapport ou du résumé appartient au Comité de surveillance.

31. *Nous recommandons*, par conséquent, que:

a) les mots au début de l'article 55 soient modifiés afin de prévoir qu'avant d'établir le contenu d'un résumé ou d'un rapport décrit à l'article 55, le Comité de surveillance consulte le directeur en vue de l'observation de l'article 37; et

b) qu'un nouveau paragraphe soit ajouté, comme suit:

La décision du Comité de surveillance à cet égard est péremptoire.